La valutazione del livello di integrità dei sistemi di protezione delle macchine, dall'analisi dei rischi ai dati affidabilistici.

INDEX

1. SCOPE

The core of the project is the development and application of a method to consider human and organization factors to be integrated with the assessment methods proposed by technical standards applied for evaluation of safety critical equipment and procedures of industrial machine.

The first target of the analysis was to test the applicability of most recent generation standards that are not yet fully acquired by different industries and to verify their effectiveness in safety assessment.

Based on the results achieved by the first phase of work, the second objective consisted of devising a method to account qualitatively and quantitatively for the human factor in the current applied standards (e.g. Failure mode and Effect analysis (FMEA), standard HazOp analysis and in Integrity Level of Safety system (SIL) analysis), verifying how a proper account of the impact of Human and Organizational Factors (H&OF) in the operational phase may provide a sensitive change in the results of the assessments.

This approach aimed at optimizing risk assessment methodologies, data and information, in order to achieve quantifiable results in the industrial domain: maximum availability, minimum unscheduled shutdowns of production, economic maintenance, minimum incident and accident, but keeping into account all relevant parameters, overlooked until now.

Our efforts are aimed at defining an improved methodological framework encompassing the integration of H&OF into safety analysis by means of quantitative risk assessment schemes.

In the integrated logical-probabilistic model will be innovative in that:

-it will be explicitly centered on the effects of abnormal and normal condition arising from human interactions with the machines and their protection systems;

- it will include a critical incorporation of all useful elements of latest advances in Human Reliability Analysis methods and an explicit focus on the capability to lead in the direction of a design improvement solution and the prioritization of interventions;

- it will include a realistic assessment of the maintenance procedures and policies adopted in the commercial companies.

Other authors [17] have proposed a model to take into account human factors in safety-critical systems considering the HF as a barrier function in the system. In these studies the operator is modeled as a safety function, i.e., sensors, logic solvers and actuator thus accordingly to the one components of a Safety Integrity Function (SIF).

Our efforts instead are aimed at defining an improved methodological framework encompassing the integration of H&OF into safety analysis by means of quantitative risk assessment schemes.

2. INTRODUCTION

The project started from a case study on a press where an accident occurred.

Through an appropriate risk analysis and reliability data a priority of interventions has been defined to reduce risks in the specific machinery under investigation. The main target of the analysis was to test the applicability of most recent generation standards, that are not yet fully acquired by different industries, and to verify their effectiveness.

Several research projects and programs on system safety engineering and quantitative risk analysis in the last 40 years offered very strong evidence of the crucial role that Human and Organizational Factors (HOFs) play in major accidents. Nevertheless, many of the models and application described in scientific literature demonstrate very limited impact on the technical standards applied for evaluation of safety critical equipment and procedures.

The standards descending from IEC 61508, developed for process plant and machinery contain requirements and recommendations for drafting, integrating and validating safety-related electrical, electronic and programmable control systems (SRECS) for systems in relation to the significant hazards they are expected to be exposed to. The reference parameter to be assessed is the Safety Integrity Level (SIL), that is a threshold availability.

SIL is closely related to reliability concept, index of intrinsic functionality of the system.

The reliability mathematically predicts the behavior of the system in foreseeable operating conditions. More clearly it expresses numerically the probability of correct operation of an apparatus during a certain period of time under certain environmental conditions, for which it was designed.

However this standards present some limitations and the analysis resulting in a SIL tends to overlook the following:

- the possible sources of missing intervention of the protection systems stemming from the interactions with the operators, during normal or abnormal conditions;
- the effect of maintenance policy and planning methodologies, e.g. through the concepts of system health management, diagnostic and prognostic and/or their integration with HOF analysis.

2.1 THE IMPORTANCE OF SAFETY RELATED TO INDUSTRIAL MACHINERY

Compliance with these standard provides one means of conformity with the specified essential requirements given in Annex I of the EC Directive 2006/42/EC, but not only.

Other benefits followed such as:

- less redundancy and more adequate and accurate choice in system architecture and consequent cost reduction;
- reduction of risks and consequent injuries;
- enhancement motivation of your staff;
- provide leverage for competitive advantage: maximum availability, minimum unscheduled shutdowns of production, economic maintenance, minimum incident and accident.

2.2 MACHINERY DIRECTIVE PRINCIPLES

Machinery Directive 2006/42/EC is a set of rules defined by European Community addressed to manufacturers but not only. The principles of the Directive must be known also by the user for a simple reason, the end users of the machine should be actively involved throughout the whole risk assessment process and should play a crucial role in ensuring an evaluation of the conditions leading to a safe operations of the equipment. The connection between Directive 2006/42/EC and IEC regulation is linked to essential requirement given in Annex I of the Directive.

Machinery means an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application.

The safety component is an element used to fulfill a safety function; the failure or malfunction of this component endangers the safety of persons.

To ensure a certain safety integrity level to safety component is therefore a indispensable requirement to comply with the regulation.

2.3 DEFINITION OF THE GOALS

The main target of the study was to test the applicability of most recent generation standards, that are not yet fully acquired by different industries, and to verify their effectiveness.

The study was focused on a hydraulic press where an accident occurred.

The fortuitous fall of the template centering tool into the mold induced the worker to bring his hands into an exposed position to fix it. Suddenly and without command activation the descent of the punch occurred, causing serious injury to the worker. The accident was the consequence of a failure in the left button of the two-hand control safety, that caused an improper contact between the conductors of the control circuit (It was as if the operator had pressed the two buttons on the two-hand control safety). A risk analysis was performed.

Based on the results achieved by the first phase of work, the second objective consists of devising a method to account qualitatively and quantitatively for the human factor in verify the Integrity Level of Safety system (SIL) called "operational SIL" which may differ from the design SIL, due to the impact of human and organizational factors (H&OF) in the operational phase. The design of automatic systems and the control of the interaction with operators have become much more complex. In particular, the consequences of an erroneous human action or of a "misunderstanding" between human beings and technologies, can have unrecoverable and dangerous consequences. Once SIL assigned to Safety-Related Electrical Control System (SRECS) for a good quality assessment to identify the possible causes and the possible consequences of the unforeseen actions identified to consider human error, was essential.

2.3.1 Why the safety standard EN IEC 61062?

The loss of the safety features of the electrical command and control systems of the machinery caused by the age of the device, lack of maintenance or improper repairs/modifications have a strong impact on possible causes of an accident. The objective of designer and end users has to be to avoid these accidents.

The choice of this standard derived from IEC 61508 that originally developed for process plants, machineries and vehicles and that contains requirements and recommendations for validating safety-related electrical, electronic and programmable control systems. In effect the EN IEC 62061 represents a sector-specific standard under IEC 61508.

The IEC 62061 describes the implementation of safety-related electrical control systems on machinery and examines the overall lifecycle from the concept phase through to decommissioning related to safety requirements. Quantitative and qualitative examinations of reliability of the safety functions form the basis.

It is intended to facilitate the specification of the performance of safety-related electrical control systems in relation to the significant hazards (see 3.8 of ISO 12100-1 [6]) of machines.

There are many situations on machines where SRECS are employed as part of safety measures that have been provided to achieve risk reduction. A typical case is the use of an interlocking guard that, when it is opened to allow access to the danger zone, signals the electrical control system to stop hazardous machine operation. Also in automation, the electrical control system that is used to achieve correct operation of the machine process often contributes to safety by mitigating risks associated with hazards arising directly from control system failures. This standard gives a methodology and requirements to:

- assign the required safety integrity level for each safety-related control function to be implemented by SRECS;
- enable the design of the SRECS appropriate to the assigned safety-related control function(s);
- integrate safety-related subsystems designed in accordance with ISO 13849 [13];
- validate the SRECS.

This standard is intended to be used within the framework of systematic risk reduction described in ISO 12100-1 [16] and in conjunction with risk assessment according to the principles described in ISO 14121 [8]. A suggested methodology for Safety Integrity Level (SIL) assignment is given in informative Annex A.

Measures are given to co-ordinate the performance of the SRECS with the intended risk reduction taking into account the probabilities and consequences of random or systematic faults within the electrical control system.

The EN IEC 62061 has been listed as a harmonised standard in the Official Journal of the EU since 31.12.2005 but it was not perfectly acquired by the stakeholders and this has been an additional source of interest.

3. THE RELIABILITY CONCEPT IN THE SAFETY STANDARD EN IEC 62061

The reliability is the probability of proper operation of a system for a specific period of time under certain conditions. The Safety Integrity Level, main concept of the technical standard, involves this concept and it is an indispensable requirement related to industrial machinery.

3.1 FUNDAMENTAL PRINCIPLES APPLIED IN THE ANALYSIS

As mentioned above this technical regulation describes the implementation of Safety-Related Electrical Control Systems (SRECS) on machinery and examines the overall lifecycle from the concept phase through to decommissioning from the point of view of reliability of the system.

For a correct application of the standard the risk must be estimated and the SIL defined for each hazard on which the risk has to be reduced through control measures.

Safety Integrity Level (SIL) is defined as a relative level of risk-reduction provided by a safety device or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance and reliability required for a Safety Instrumented Function (SIF).

The SRECS achieves the defined SIL on the basis of architectural constraints which permit to ensure a Probability of a Dangerous Failure (PDF) not too high.

In fact the probability of a dangerous failure of each Safety-Related Control Function (SRCF) shall be equal to or less than the failure threshold value defined in the specification of the safety requirements.

SIL	PFH
3	$\geq 10^{-9}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 1: Intervals of the average probability of a dangerous failure per hour (PFH) corresponding to the safety integrity levels (IEC 62061:2005).

The safety standard IEC 62061 shows a simplified approach to the estimation of probability of dangerous random hardware failures for a number of basic subsystem architectures and gives formulae that can be used for subsystems assembled from either low complexity subsystem elements or complex subsystem.

The formulae are a simplification of reliability analysis theory and are intended to provide estimates that are biased towards the safe direction. The precondition for the validity for all formulae given in this sub-clause is that $1 >> \lambda \times T_1$, where λ is failure rate (1/h) and T_1 is the smaller of the proof test interval or the lifetime, and the subsystem is operating in the "high demand or continuous mode". Therefore, the following basic equations can be used: $\lambda = 1/MTTF$ where MTTF means Mean Time To Failure.

3.1.1 Architecture of safety related control function

The probability of dangerous failure of each subsystem due to random hardware failures to perform the allocated function blocks shall be estimated taking into account:

a) the architecture of the subsystem as it relates to the allocated function blocks under consideration;

b) the rate of failure of each subsystem element in any modes which would cause a dangerous failure of the subsystem but which are detected by diagnostic tests;

c) the rate of failure of each subsystem element in any modes which would cause a dangerous failure of the subsystem which are undetected by the diagnostic tests;

d) the susceptibility of the subsystem to common cause failures which would cause a dangerous failure of the subsystem;

Note 1: Where comparison of redundant components is used for fault detection, failure of the fault detection means can occur when the redundant components fail at the same time in the same mode. This can occur due to a common cause referred to as a common cause failure (CCF) that is expressed as a beta (ß) factor. A simplified approach to estimate the susceptibility to common cause failures is given by Annex D of the standard.

e) the diagnostic coverage of the diagnostic tests and the associated diagnostic test interval;

f) the intervals at which proof tests are undertaken to reveal dangerous faults which are undetected by diagnostic tests and/or the mission time of the subsystem element(s) which should not be exceeded in order to maintain the validity of the information given in items b) and c);

g) the repair times for detected faults where the subsystem is designed for online repair.

The standard provides four different type of architectures:

1. Basic subsystem architecture A: zero fault tolerance without a diagnostic function.

   In this architecture, any dangerous failure of a subsystem element causes a failure of the SRCF. For architecture A, the probability of dangerous failure of the subsystem is the sum of the probabilities of dangerous failure of all subsystems elements (Figure 1):

   $\lambda_{DssA} = \lambda_{De1} + ...+ \lambda_{Den}$

   $PFH_{DssA} = \lambda_{DssA} \times 1h$

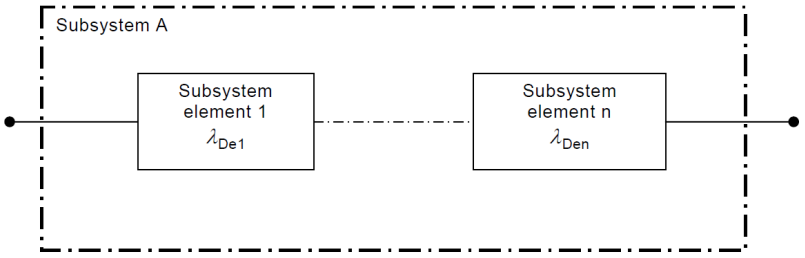


Figure 1: Subsystem A logical representation

2. Basic subsystem architecture B: single fault tolerance without a diagnostic function.

   This architecture is such that a single failure of any subsystem element does not cause a loss of the SRCF. Thus, there would have to be a dangerous failure in more than one element before failure of the SRCF can occur. For architecture B, the probability of dangerous failure of the subsystem is (Figure 2).

   $\lambda_{DssB} = (1 - \beta)2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$

   $PFH_{DssB} = \lambda_{DssB} \times 1h$

   where

   T_1 is the proof test interval or lifetime whichever is the smaller.

   β is the susceptibility to common cause failures.

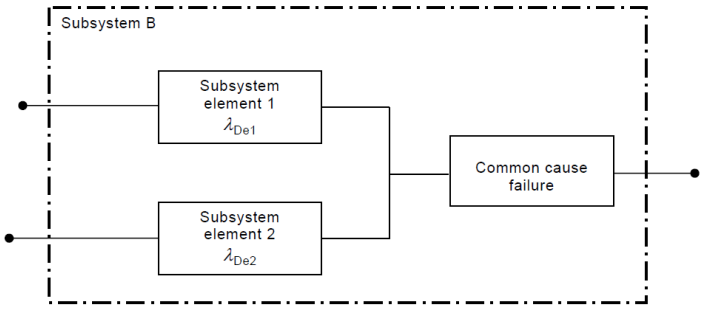


Figure 2: Subsystem B logical representation

3. Basic subsystem architecture C: zero fault tolerance with a diagnostic function.

   Any undetected dangerous fault of the subsystem element leads to a dangerous failure of the SRCF. Where a fault of a subsystem element is detected, the diagnostic function(s) initiates a fault reaction function. For architecture C, the probability of dangerous failure of the subsystem is (Figure 3):

$\lambda_{DssC} = \lambda_{De1} (1 - DC1) + ...+ \lambda_{Den}(1 - DC_n)$

$PFH_{DssC} = \lambda_{DssC}$ x 1h

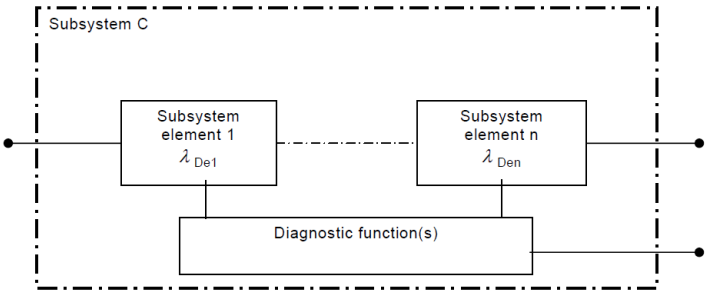


Figure 3: Subsystem C logical representation

4. Basic subsystem <u>architecture D</u>: single fault tolerance with a diagnostic function(s).

   This architecture is such that a single failure of any subsystem element does not cause a loss of the SRCF (Figure 4Figure 4, where

   T_2 is the diagnostic test interval;

   T_1 is the proof test interval or lifetime whichever is the smaller.

   β is the susceptibility to common cause failures; $\lambda_D = \lambda_{DD} + \lambda_{DU}$; where λ_{DD} is the rate of detectable dangerous failures and λ_{DU} is the rate of undetectable dangerous failure.

   $\lambda_{DD} = \lambda_D$ x DC

   $\lambda_{DU} = \lambda_D$ x (1 – DC)

   <u>For subsystem elements of different design:</u>

   λ_{De1} is the dangerous failure rate of subsystem element 1;

   DC_1 is the diagnostic coverage of subsystem element 1;

   λ_{De2} is the dangerous failure rate of subsystem element 2;

   DC_2 is the diagnostic coverage of subsystem element 2.

   $\lambda_{DssD} = (1 - \beta)2 \{[\lambda_{De1}$ x λ_{De2} x $(DC_1 + DC_2)]$ x $T_2/2 + [\lambda_{De1}$ x λ_{De2} x $(2 - DC_1 - DC_2)$] x $T_1/2 \} + \beta$ x $(\lambda_{De1} + \lambda_{De2})/2$

   $PFHDssD = \lambda_{DssD}$ x 1h

   <u>For subsystem elements of the same design:</u>

   λ_{De} is the dangerous failure rate of subsystem element 1 or 2;

   DC is the diagnostic coverage of subsystem element 1 or 2.

$\lambda_{DssD} = (1 - \beta)2 \{[\lambda_{De2} \times 2 \times DC] \times T_2/2 + [\lambda_{De2} \times (1 - DC)] \times T_1\} + \beta \times \lambda_{De}$

$PFH_{DssD} = \lambda_{DssD} \times 1h$

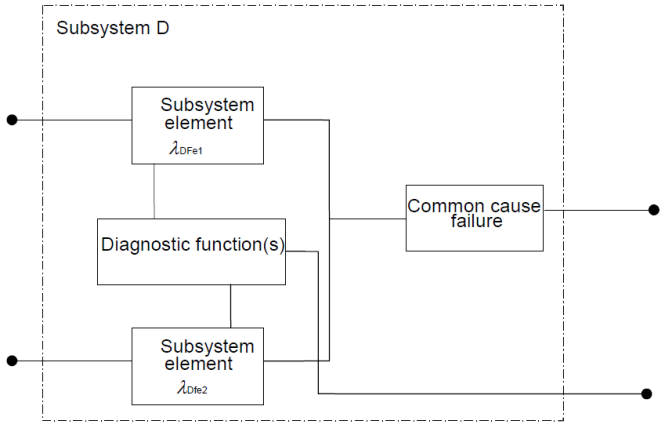


Figure 4: Subsystem D logical representation

Two of these type of architectures were applied in this research project (chapter 4 paragraph. 4.1.4).

4. CASE STUDY

The range of machines to work metal sheets is very large. Among all types of existing machines the study is focused on a hydraulic press where an accident occurred.

A worker in charge of stamping and bending steel handles for pots, was injured. The fortuitous fall of the template centering tool into the mould induced the worker to bring his hands into an exposed position to fix it. Suddenly and without command activation the descent of the punch occurred, causing serious injury to the worker. The accident was the consequence of a failure in the left button of the two-hand control safety, that caused an improper contact between the conductors of the control circuit.

Analysis of the electrical circuit diagram showed that this failure was enough to start a machine cycle: it was as if the operator had pressed the two buttons on the two-hand control safety.

To the machine involved in the accident a risk analysis technique has been applied in order to identify the lacking protective means and thus priority of interventions to reduce risks.

4.1 RISK ANALYSIS IN ACCORDANCE WITH THE SAFETY STANDARD

The following diagram (Figure 5) shows the process of risk assessment step by step.

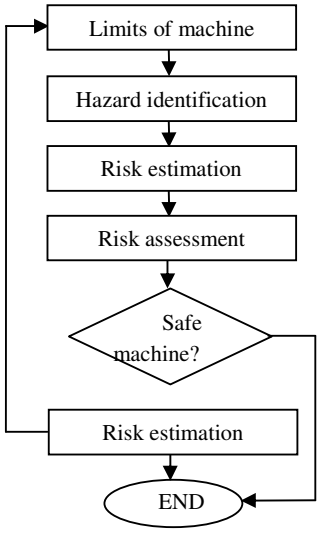


Figure 5: Risk assessment method

4.1.1 HazID Analysis

A risk assessment should include a look at each functional part in turn, making sure that every mode of operation and all phases of use are properly considered, including the human-machine interaction in relation to the identified functions or functional parts. For this reason the Hazard Identification approach (HazID) was chosen to investigate the criticalities of the tool (Lees,1996). This kind of analysis is the starting point for a detailed risk assessment.

The approach is divided into two phases: the former developing the description of the functions performed by the system, the latter is oriented to analyze one by one those functions, to highlight possible deviations, their causes and the consequent effect (Table 2).

Identifying all the elementary functions and analyzing then allowed to assess the risk index for each of them, thereby highlighting not tolerable one.

Main Function	Elementary Function	Hazard/Deviation of Function	Cause	Consequence

Table 2: Hazard identification

In accordance with EN ISO 14121 [8] the sequence of analysis was to:

- establish the limits and the intended use of the machinery;
- identify the hazards and any associated hazardous situation;
- evaluate the risk and decide on the need for risk reduction.

In a hydraulic press the process basically consists in transforming a flat metal sheet in a concave body by means of the coordinated action of a punch and a blank holder.

The following life cycle phases of the machine can be identified:

- Assembly
- Installation
- Starting
- Processing cycle
- Facility
- Safety systems
- Maintenance
- Decommissioning
- Disposal

In each phase different hazards has been identified and the most significant are: electrical, for direct or indirect contact; contact with tools; gravity fall of the slide/ram; accidental start of the machine; increased pressure in the hydraulic circuit.

In table of Annex 12.4 extracted from the HazId analysis template (Annex 12.1), the more critical events are reported. These deviations can cause different consequences and in the worst case: crushing, shearing or amputation of fingers.

HazId analysis results showed that the more hazardous area in hydraulic presses is the tools area on the front side of the machine and preventive measures have to be taken to deal with the relevant hazards, as stated also by technical regulations.

One of the most critical phases revealed by the analysis is the use of the machine in manual mode cycle.

Moving die cushions, blanking holders and work piece ejectors shall be safeguarded.

During the verification of compliance of the press, evidence came out that the failure of the button was an event entirely predictable and quite common statistically. Nowadays, in accordance with the requirements of EN 693:2009, the control circuit of the press must be equipped with adequate safety protection that puts in safe the machine in case of failure.

If the old machine had had a two hand control devices more reliable and a safeguarding using an electro-sensitive protective equipment (ESPE) probably the injury would not have occurred.
But at the time of the accident, however, these requirements were not requested by law and the machine was correctly designed according to the standards of that period.
The whole risk analysis underlines that the most dangerous operation phases are “Setting tools”, “Starting loop for material processing” and “Feeding and loading raw materials”.
To reduce the hazard of coming into contact with the tool the appropriate protective system is the addition of a safeguarding.
The safety standard EN 693:2009 for Hydraulic presses requires that the safety functions, “two hand control devices” and “safeguarding”, are installed with a specific category that correspond to a certain level of safety integrity.
The categories are the instruments to achieve the Safety Integrity Level (SIL); they establish the required behavior of Safety-Related Parts of Control System (SRP/CS) compared to its resistance to damage. In category 1 to improve resistance to damage is achieved primarily through the selection and application components. In categories 2, 3 and 4 the best performance for a specific safety function is achieved mainly by improving the structure of the SRP/CS.

4.1.2 Risk assessment and SIL assignment

Through an appropriate risk analysis and reliability data a priority of interventions has been defined to reduce risks in the specific machine under investigation.
The following figure (Figure 5) shows an example of a practical way of carrying out a risk assessment leading to the estimation of a SIL requirement for each Safety-Related Electrical Control System (SRECS). This methodology should be performed for each risk that can be reduced by a safety-related control function and implemented by a SRECS.

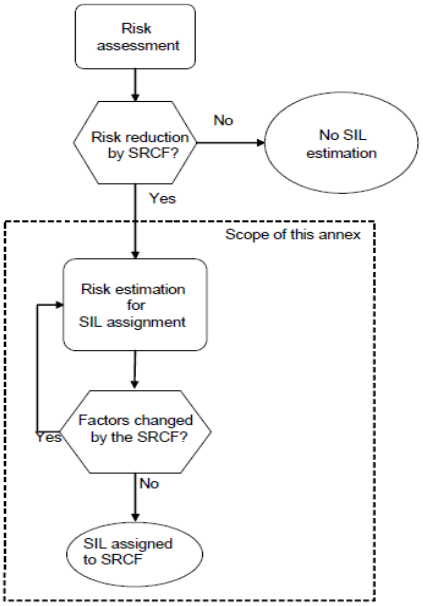


Figure 6: Workflow of SIL assignment process

Risk estimation should be carried out for each hazard by determining risk parameters that should be derived from the following:

- Severity of harm, Se
- Probability of occurrence of that harm expressed by Class indicator (Cl) which is function of:
  - frequency and duration of the exposure of persons to the hazard, Fr;
  - index of probability of occurrence of a hazardous event, Pr;
  - possibilities to avoid or limit the harm, Av.

$$Cl = Fr + Pr + Av$$

Using the Table below (Table 3), where the severity (Se) row crosses the relevant column Class (Cl), the intersection point indicates whether action is required. The black area indicates the SIL assigned as the target for the Safety-Related Control Function (SRCF). The lighter shaded areas should be used as a recommendation that other measures (OM) should be used. The white box indicates that the danger is properly treated and therefore complies with the requirement of the Machinery Directive.

Severity (S_e)	Classe (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Table 3: Matrix of SIL assignment

Example: for the crushing hazard in tools' dangerous area the following values are assigned (EN ISO 14121): Se= 4 irreversible consequence: death, losing an eye or arm; Fr= 5: the frequency of exposure is ≤ 1 h; Pr=3 and Av= 3: the operators are trained and know the criticality of the machine, but failure of the machine is not always predictable in time to avoid; then :

Cl = Fr + Pr + Av = 5 + 3 + 3 = 11

Using the matrix of SIL assignment (Table 3), this would lead to a SIL 3 being assigned to the SRCF that is intended to mitigate against the specific hazard.

For an up-to-date hydraulic press, often SIL is already assigned by the standard law of type C through the use of categories; when SIL is not indicated it is correct then to proceed as in the example.

Moreover, not all machines have a specific technical standard: for this reason it will be useful to know how to apply this method.

In the case of a hydraulic press safety standard at point 5.3.15 requires that active opto-electronic protective devices (AOPD) must be conform to type 4 of EN 61496-1:1997 which is equivalent to a category 4 that corresponds to a SIL 3, as achieved through the risk analysis of the example.

SIL 3 means that the system shall be redundant and monitored (R&M), where a fault occurs in one channel of a two channel control system, so that the other channel remains operative.

4.1.3 SIL verification trough Safety Standard EN IEC 61062

One of the main purposes of functional safety analysis is the determination of required safety integrity level (SIL) of the safety-related functions to be realized by safety-related systems.

Safety integrity is a fundamental concept in IEC 62061 and it is defined as the "probability of a safety-related system satisfactorily performing the required safety function under all stated conditions within a specified period of time".

The standard defines three safety integrity levels, where SIL 3 is the highest level and SIL 1 is the lowest. Each level corresponds to an interval of the probability of a dangerous failure per hour (PFH) as shown in the Table below (Table 4).

SIL	PFH
3	$\geq 10^{-9}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 4: Intervals of the average probability of a dangerous failure per hour (PFH) corresponding to the safety integrity levels (IEC 62061:2005).

The safety functions identified from the risk analysis are divided into safety sub-function; these safety sub-functions are than assigned to actual devices, called subsystems and subsystem elements.

A safety-related control system is made up of several subsystems. The safety-related characteristics of these subsystem are described through the following parameters:

- SILCL: SIL claim limit, (maximum SIL that can be claimed for a SRECS subsystem in relation to architectural constraints and systematic safety integrity).
- PFHD: Probability of dangerous failure per hour
- T_1: lifetime

These subsystems may in turn be made up of various interconnected subsystem elements (devices) with parameters to calculate the subsystem's corresponding PFHD value.

Safety-related parameters for subsystem elements (devices) are:

- λ: Failure rate; for wearing elements: described through the B10 value that is the expected time for 10% of the sample fails.
- SFF: Safe failure fraction, it is the fraction of the overall failure rate of a subsystem that does not result in a dangerous failure.

On electromechanical devices the failure rate is indicated by the manufacturer as a B_{10} value, based on the number of cycles. The time-based failure rate and lifetime must be determined through the switching frequency for the respective application.

Internal parameters to be established during design/construction for a subsystem including subsystem elements are

- T_2: Diagnostic test interval
- β: Susceptibility to common cause failure
- DC: Diagnostic coverage
- PFH_D: The PFH_D value of the safety-related control system is calculated by adding the subsystems' individual PFH_D values.

4.1.4 SIL computation for the safeguarding of Hydraulic press complies with safety standards

Once SIL has been assigned to Safety-Related Electrical Control System (SRECS), it is fundamental to calculate the SIL associated to that component and to verify if it is equal to the previously assigned SIL.

As mentioned above, the major danger zone on hydraulic press is the tools area and preventive measures shall be taken to deal with the relevant hazards.

Mode of production, mode of cycle initiation and mode of operation are fundamental to understand which safeguarding methods should be adopted.

Guard system has to reduce the risk as far as possible, considering the significant hazards and the mode of production.

The selected combination of safeguarding measures shall protect all exposed persons.

With the introduction of European standards of safety all working sides of the press must be carefully protected (see Table 5).

Safety objective	Safety measures	Compliance with the Machinery Directive
Accessibility to moving parts: the front	The front of the machine is protected by light barriers	1.3.7 Risks associated with moving tools 1.4 Required characteristics of guards and protective devices

Table 5: Compliance with the Machinery Directive

The light barriers are installed to protect the area from possible danger or accidental access.

The light barrier is connected to a safety circuit that generates a safe shutdown of the beam through the solenoid safety.

The identified SRCF is: “during operation, the photocell works in guard position, thus interrupting the range of the photocell the press stops any movement of the machine and it is placed in security conditions”.

The SRCF has been described through functional blocks.

As seen above, the assigned SIL for this SRCF through the risk analysis is 3 and also safety standard recommended category 4 corresponding to a SIL 3.

To achieve the required SRCF the choice is needed of a Safety-Related Electrical Control System (SRECS) designed accordingly.

Decomposition to a structure of functional blocks (FB) is showed below (Figure 7).

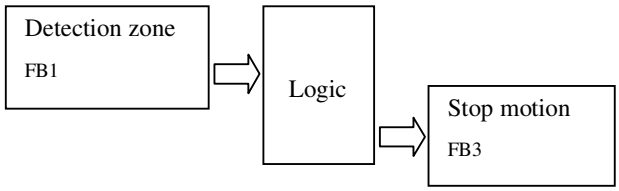


Figure 7: Functional block

Once identified functional blocks, subsystems (SS) were chosen (Figure 8).

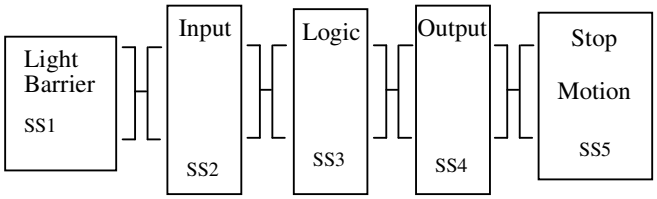


Figure 8: Subsystem composition

In this example, the target failure value for the safety-related control function is SIL 3 this is equivalent to a probability of dangerous failure per hour (PFH_D) in the range ≥ 10-9 to < 10-7.

The probability of dangerous random hardware failure of the SRECS (PFH_{DSRECS}) is the sum of the probabilities of dangerous failure per hour of all subsystems ($PFH_{D1}$to PFH_{Dn}) involved in the performance of the safety-related control function:

$PFH_{DSRECS} = PFH_{D1} + ...+ PFH_{Dn}$

Each subsystem has its own well-defined architecture.

The architectures of subsystem Sensor and Logic are all based on logic 1oo2 (1 out of 2) and the basic architecture is of type B (Figure 9).

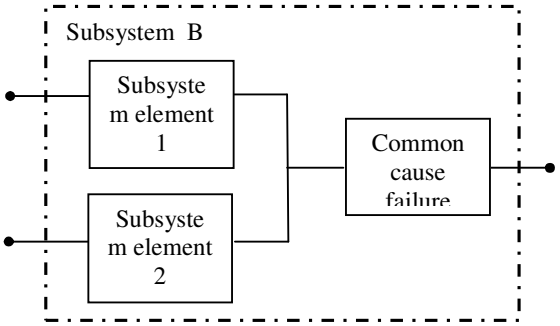


Figure 9: Subsystem B logical representation

This architecture is such that a single failure of any subsystem element does not cause a loss of the SRCF. Thus, a dangerous failure in more than one element has to occur before the failure of the SRCF happens. For architecture B, the probability of dangerous failure of the subsystem is:

$\lambda_{DssB} = (1 - \beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssB} = \lambda_{DssB} \times 1h$

where:

T_1 is the proof test interval or lifetime whichever is the smaller;

β is the susceptibility to common cause failures. Where a redundant architecture is used to achieve the required probability of dangerous random hardware failure of a subsystem and a Common Cause Failure (CCF(s)) can remove the effect of that redundancy, the probability of dangerous random hardware failure based on the probability of occurrence of the common cause shall be added to the probability of dangerous random hardware failure of a subsystem based on the use of redundancy.

For the Actuator an architecture of type D was provided (Figure 10).

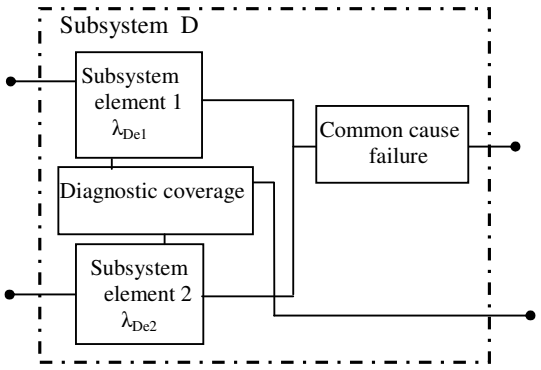


Figure 10: Subsystem D logical representation

This architecture is such that a single failure of any subsystem element does not cause a loss of the SRCF, where

T_2 is the diagnostic test interval;

T_1 is the proof test interval or lifetime whichever is the smaller;

β is the susceptibility to common cause failures;

$\lambda_D = \lambda_{DD} + \lambda_{DU}$; where λ_{DD} is the rate of detectable dangerous failures and λ_{DU} is the rate of undetectable dangerous failure.

λ_{De1} is the dangerous failure rate of SS element 1;

DC_1 is the diagnostic coverage of SS element 1;

λ_{De2} is the dangerous failure rate of subsystem element 2;

DC_2 is the diagnostic coverage of SS element 2.

For architecture D, the probability of dangerous failure of the subsystem is:

$\lambda_{DssD} = (1 - \beta)^2 \{[\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2)] \times T_2/2 + [\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2)] \times T_1/2 \} + \beta \times (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssD} = \lambda_{DssD} \times 1h$

In this case study the data have been provided directly by the manufacturer and are:

Light barrier: $PFH_D = 3.79 \times 10^{-9}$

Input: $PFH_D = 2.90 \times 10^{-10}$

PLC: $PFH_D = 9.20 \times 10^{-9}$

Output: $PFH_D = 8.60 \times 10^{-10}$

Instead for the actuator PFH_D has been calculated with formulae provided by the standard.

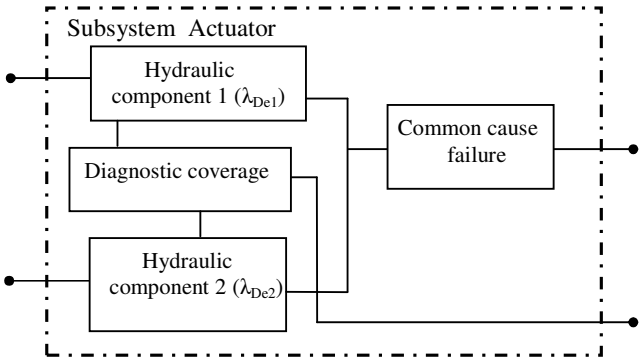


Figure 11: Subsystem Actuator logical representation

For subsystem elements of the same design the formula becomes:

$\lambda_{Dss5} = (1 - \beta)^2 \{[\lambda_{De2} \times 2 \times DC] \times T_2/2 + [\lambda_{De2} \times (1 - DC)] \times T_1\} + \beta \times \lambda_{De}$

where:

λ_{De}= 7.64x10^{-7}

β = 0.10

T_2 = 0.5

T_1 = 20 years

The results is λ_{Dss5} = 7.69 x 10^{-8}

Actuator: PFH_D = 7.69 x 10^{-8} x 1h

The total PFH_D of SRECS will therefore composed as follows (Figure 12):

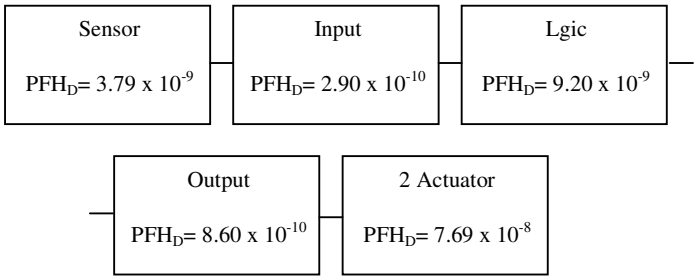


Figure 12: Block diagram

PFH_{DSRECS} = 3.79x10^{-9} + 2.90x10^{-10} + 9.20x10^{-9}+ 8.60x10^{-10}+7.69x10^{-8}= 9.11x10^{-8} →SIL 3

The realized SRECS is suitable for SRCF (SIL3).

4.1.5 Results of the application

This case study has shown that the performance of a safety instrumented system in the operational phase is influenced by many factors; not only by the system design and the related testing and maintenance strategies, but also by the operating conditions.

A significant part of all industrial accidents is caused by unanticipated actions of people during operation and maintenance, and the organizational perspective on safety shows that these human errors often are caused by aspects of the organization and the working environment.

It became clear that human and organizational factors could affect the performance of safety instrumented systems and may threaten the achieved SIL. For this reason the future challenge in this research was to take in to account the human factor in the risk assessment used as a base for assigning integrity levels of safety systems (SIL) to the identified security functions.

The approach will give a prediction of the achieved SIL during operation, called operational SIL (chapter 5) which may differ from the design SIL, due to the impact of human and organizational factors in the operational phase.

5. LIMITS OF THE STANDARD

The technical regulation IEC related to safety standard of machinery is not completely exhaustive for the aspects of detail affecting the interface human being-machine.

Likely one of the possible causes is the fact that the concept of SIL, that derived from IEC 61508 originally developed for process plants (actually mostly automated) has been passed on sectors most closely linked to human activity.

5.1 HUMAN FACTOR FOR "SIL" CALCULATION

The standard IEC 62061 for instance contains requirements and recommendations for drafting, integrating and validating Safety-Related Electrical, electronic and programmable Control Systems (SRECS) for machinery in relation to the significant hazards they are expected to be exposed to. However no indication is provided in respect to the possible sources of hazards for the Safety Integrity Level (SIL) to be evaluated stemming from the interactions with the operators, during normal or abnormal conditions.

The effects of human error on system performance could change significantly the results of risk assessment. The standards doesn't provide any clear approach to perform risk analysis taking into account human factors.

5.1.1 Results from the first step of analysis and subsequent development

Actually, many studies show that erroneous human actions are the predominant causes of relevant incidental events.

The results from the first step of the analysis and other surveys as BGIA study (paragraph 5.1.2) suggests the need of properly assessing of these risks attributable to human error and the need of reducing system vulnerability to human error impact.

The core of the project is the development and application of a method to consider human and organization factors to be integrated with the assessment methods proposed by technical standards applied for evaluation of safety critical equipment and procedures.

5.1.2 BGIA Study

Institutions for statutory accident insurance and prevention (Germany and Switzerland) through a survey on a sample of 1605 workers between the years 1996 and 2000, has investigated the scale of tampering with machinery safety to obtain a specific analysis of the reasons of that. The study was supported by the data shown below (Figure 13).

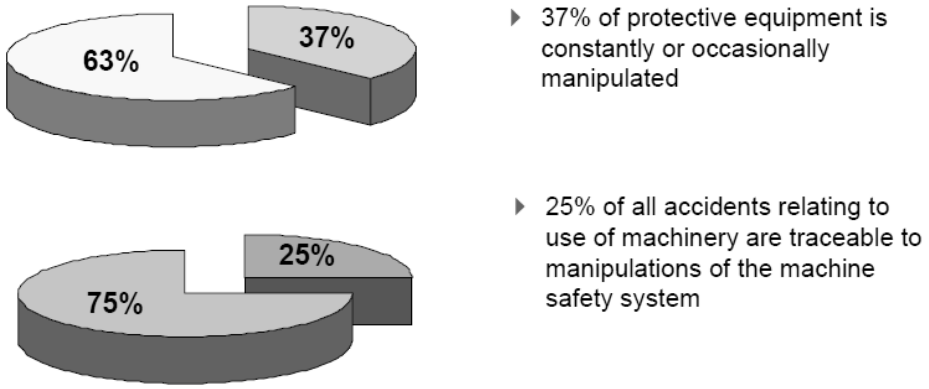


Figure 13: Statistics of accidents relating to use of machinery

The investigation revealed that the reasons why the operator by-pass the safety devices are due to comfort, time gain, simplification of the work and achievement pressure, emphasizing once again how important it is to take into account certain problems (human factors) right from SRECS design stage.

The study describes the way to by-pass the safety devices for each type of safe guarding: manipulation of electro-mechanical devices by bridging, fixed guarding tampering or removing, manipulation of optoelectronic protection devices by repositioning, etc.

General findings of BGIA study show that:

- 60% of manipulations apply to machinery which was generally in compliance with generally in accordance with the technical requirements of the standards;
- 40% during manual setting mode and observation;
- 37% either permanent or temporary bypassed;
- 25% during safety system in override mode;
- 14% of machines covered in the study are manipulated constantly;
- 51% of all observed manipulations result in accidents;
- 34% of the companies tolerate the manipulation of the machines.

The last statement shows once again how some users ignore the existence of some standards also if the regulations were already issued.

BGIA study was a good tool to identify improper human behaviors during the analysis.

5.1.3 "Operational SIL"

Human and organizational factors affect the performance of safety instrumented systems during operation and may threaten the achieved SIL, but this is usually not explicitly accounted for.

Therefore, based on the results achieved by the first phase of work, the second step of the research consisted of developing an approach to assess the impact of human and organisational factors on the achieved SIL in the operational phase of safety instrumented systems (*operational SIL*). The objective consisted of devising a method to account qualitatively and quantitatively for the human factor in the current applied standards (e.g. Failure mode and Effect Analysis (FMEA), standard HAzOp analysis and in Integrity Level of Safety system (SIL) analysis), verifying how a proper account of the impact of human and organizational factors (H&OF) in the operational phase may provide a sensitive change in the results of the assessments.

5.1.4 Integrating human factors in a safety analysis with an engineering approach

Once modeled the logic of the system and man-machine interface we had to proceed with quantitative assessment of the Human Error Probability (HEP) and finally to calculate Probability of Dangerous Failure per Hour (PFH_D) of the SRECS in order to assess the "operational SIL". If it is minus or equal to SIL assigned then SRECS will be suitable for Safety-Related Control Function otherwise it will be necessary to carry out a failure reduction analysis and to repeat IROA analysis (Figure 14).

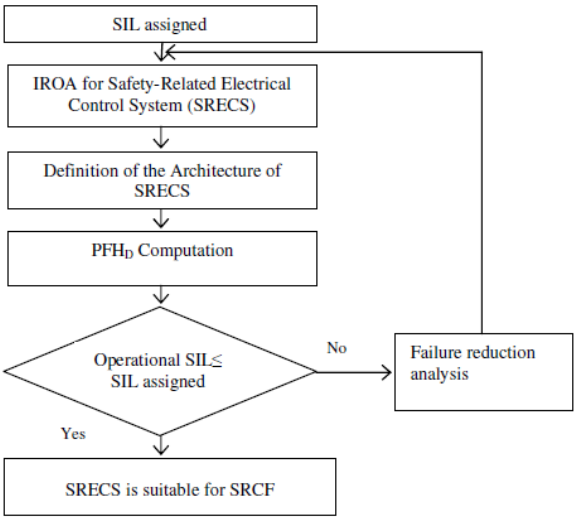


Figure 14: Flowchart Operational SIL verification

The observations and results from the first target of the analysis led to try to define a method to consider human and organizational factors to be integrated with the assessment methods proposed by technical standards applied for evaluation of safety critical equipment and procedures.

In the logical-probabilistic model the following element of innovation has been considered:

• it was explicitly centered on the effects of abnormal and normal condition raising from human interactions;

• it included a critical incorporation of all useful elements of latest advances in Human Reliability Analysis methods and an explicit focus on the capability to lead in the direction of a design improvement solution and the prioritization of interventions.

Incorporating human factors (HFs) into safety analyses is rather difficult and complex exercise. For the project purpose we needed of a methodological framework which could ease the way in which safety analysis may account for human an organizational factors (H&OF) since the early stages of the analysis.

For these reasons the Integrated Recursive Operability Analysis (IROA) was chosen as a first attempt to reach the second goal of the study.

A further evidence of the importance of taking into account the integration of human factor in risk analysis was given by the case study carried out by me at Trinity College of Dublin where another approach was applied (Chapter 6 paragraph 6.4.1). In that occasion the Risk Assessment was performed using an ad hoc Failure Mode and Effects Analysis (FMEA) template where the functional analysis included the human tasks as well as a technical aspects.

Further the risk levels associated to each possible failure mode was obtained using the risk matrix proposed by the Military Standard MIL-STD-882. The overall method aimed at providing the assessment of a Risk Level similar to the Safety Integrity Level evaluation required by standards descending from IEC 61508 (originally developed for process plants, machineries and vehicles contain requirements and recommendations for validating safety-related electrical, electronic and programmable control systems). The results of the analysis proved that a proper account of the impact of human factors related issues provide a sensitive change in the overall risk level associated to the installation.

5.1.5 Two possible approach for the new methodology

For the reasons explained above, to verify how a proper account of the impact of human and organizational factors in the operational phase provides a sensitive change in the result of reliability analysis, the first approach to take into account was IROA methodology.

This approach is similar to that of the classic Recursive Operability Analysis, but with some added features that enable one to accommodate systematically H&OF into the process (Chapter 6 paragraph 6.1).

This first attempt to apply IROA methodology shows that this type of analysis highlights the position where in depth human factor analysis must be carried out. It is a qualitative approach as well, but more complete and systematic than the HazId methodology applied in the first phase of the study.

Once the point is identified in which the human erroneous action may occur it will be necessary to insert the study of human factors and the assessment Human Error Probability (HEP).

Our efforts are aimed at defining an improved methodological framework encompassing the integration of H&OF into safety analysis by means of quantitative risk assessment schemes.

In order to do that the suggested tool is the Integrated Dynamic Decision Analysis (IDDA) [40], [41], [42], [43]. This tool allows modeling the logic of a complex system; it provides a representation of all the possible alternative states into which the system could evolve, as a real logical and temporal sequence of events.

IDDA integrated with Task Analysis (TA) (Chapter 6, paragraph 6.4) could allow to obtain a detailed quantitative analysis of human factors directly during the same risk assessment.

Both approach will be pursued in this study.

6. LITERATURE SURVEY AND FIRST ATTEMPTS TO APPLY NEW METHODOLOGICAL APPROACHES

Following a thorough investigation in literature about methods of analysis that would allow to take into account the human factor in risk assessments, in this chapter some methodological approaches among those studied are presented and applied to the case study of press. The results obtained by the applications afterwards have allowed to define the final integrated approach presented in chapter 7.

6.1 IROA ANALYSIS APPROACH

Recent development of Hazard and Operability Analysis (HAZOP) approaches aimed at including human and organizational factors and a way to reach this purpose was the IROA framework.

This methodology is similar to that of the classic Recursive Operability Analysis, but with some added features that enable one to accommodate systematically H&OF into the process.

The main frame of the IROA is still made up of two blocks (Figure 15).

According to the inhibit concept, the former block is devoted to the identification of those hazards that drive the system out of control, while the latter is conceived to modeling the effectiveness of protective systems.

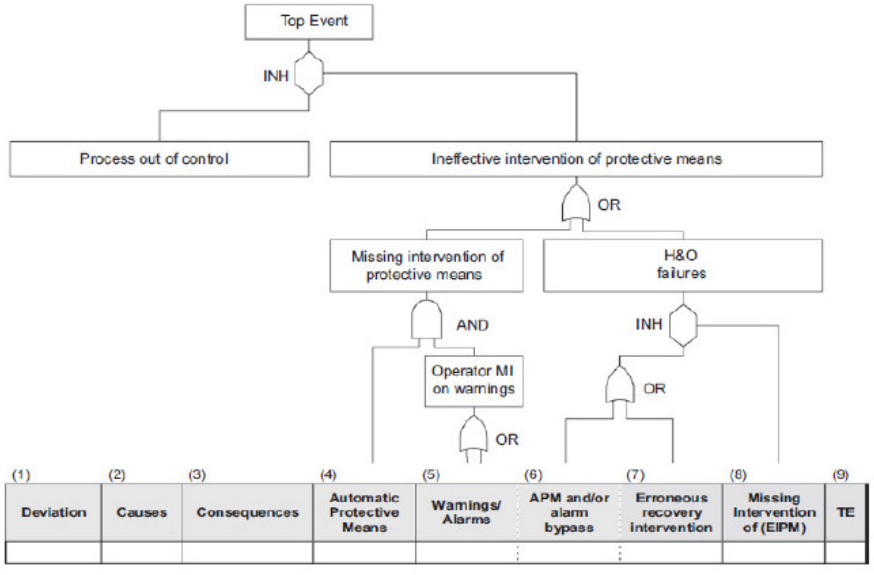


Figure 15: IROA framework

The first block, i.e., that grouping column 1–3 in Figure 15, is devoted to the identification of those primary events that leads the system out of control. In this part of the analysis even human failures are now accounted for in an integrated fashion together with technological ones. In particular, human interventions in this block have to be modeled as pre-initiators of events, meaning those acts that contribute to let the system's components to fail or be in an undetected failing state. In the IROA scheme pre-initiating human failures are modeled, together with the technological ones, in column 2 with the aim of unveiling primary human-related root causes.

The second block, that grouping column 4–9 in Figure 15, instead, is devised to identify and accommodate post-initiator human interventions, i.e., those human actions that contribute either to prevent the dangerous transient to further proceed to TE or to worsen it by accelerating its occurrence (co-causes).

In the IROA scheme the Top Event (TE) occurs if, and only if, there is an ineffective intervention of protective means. This definition allows for the accounting of the dynamic process of recovery in which human intervention plays a key role.

There is a real interpenetration and collaboration between technology and humans, making the system much safer. The failure occurs actually only when the intervention of both the automatic protective means (APM) and humans fail.

In the IROA methodological frame the trade-off between an optimal human–technology system and a bad one is modeled by attributing the ineffective intervention of protective means to the following two main causes:

• MI of protective means and

• human failure.

In the IROA concept, the human failure to recover has to be taken into account in two different cases:

• if the alarm system fails or the operator fails to ‘‘detect’’ it or another form of indication (misreading, misjudging, etc.), or

• if the plant is left without Engineered Safety Features (ESFs), due to their by-passing.

In both cases, a missing or ineffective intervention of Erroneous Intervention of Protective Means (EIPM) can be considered, and if its missing or ineffective intervention occurs, it will bring up directly to the ineffective intervention of protective means, i.e., fail to stop the wrong action.

6.1.1 Detailed analysis applied on the case study

For each critical event detected by HazId analysis in a specific scenario as material load or tool change phase, we tried to apply IROA to take into account human and organizational factors and the way in which workers could by-pass the safety devices to calculate "operational SIL" and compare it with assigned and verified SIL according to safety standard.

In this application we have considered as before the case of hydraulic press but unlike the first step of the project we have considered a machinery of last generation updated with current developments in technology and with all required safety devices included.

We present an extract related to crushing hazard in tools' dangerous area during the setting tools phase (Figure 16). From the analysis the worst case of accident is limb amputation if the automatic protective means fails and if the operator fails the recovery intervention.

The main cause of the top event seems to be the accidental starting of the machine and the analysis has been reflected in the construction of the logic tree presented below (Figure 17).

Deviation	Causes	Consequences	Automatic Protective Means (APM)	Warnings/ Alarms	APM and/or alarm bypass	Erroneous or Ineffective recovery intervention	Missing Intervention of EIPM	TE
Contact with tools	1. Accidental starting of the machine 2. Fall under gravity of the beam that holds the punch 3.Failure of ending stroke	Injury, compression, shearing, upper limb amputation (in some cases death)						
1.Accidental starting of the machine	4. Faulty contactor of two-hand control devices, all the contacts remain in the energized position *A third person operates the command without noticing a colleague who has his hands in the machine Erroneous setting of the selector switches key operated Restore electricity supply after a break	Contact with tools	MI Light barrier		Light barrier	Erroneus repositioning of light barrier, no appropriate safety distance Erroneus manual reset of the safety system		Limb amputation
4. Faulty contactor, all the contacts remain in the energized	*Short circuit due to improper contact between cables Improper use of two-hand control device	Contact with tools						

position	5. Wrong cable connection							
5. Wrong cable connection	*Wrong electric diagrams *Human error (può derivare dalla manutenzione o dall'installazione della macchina)	Contact with tools						
2. Fall under gravity of the beam that holds the punch	6. Failure of hydraulic system *Mechanical failure	Contact with tools						
6. Failure hydraulic system	*Failure of pressure relief valve *Failure of pressure exhaust valve *Failure of restraint valve	Contact with tools						
3.Failure of ending stroke	*Failure to open the electrical contacts	Contact with tools						

Figure 16: IROA framework for setting tool phase

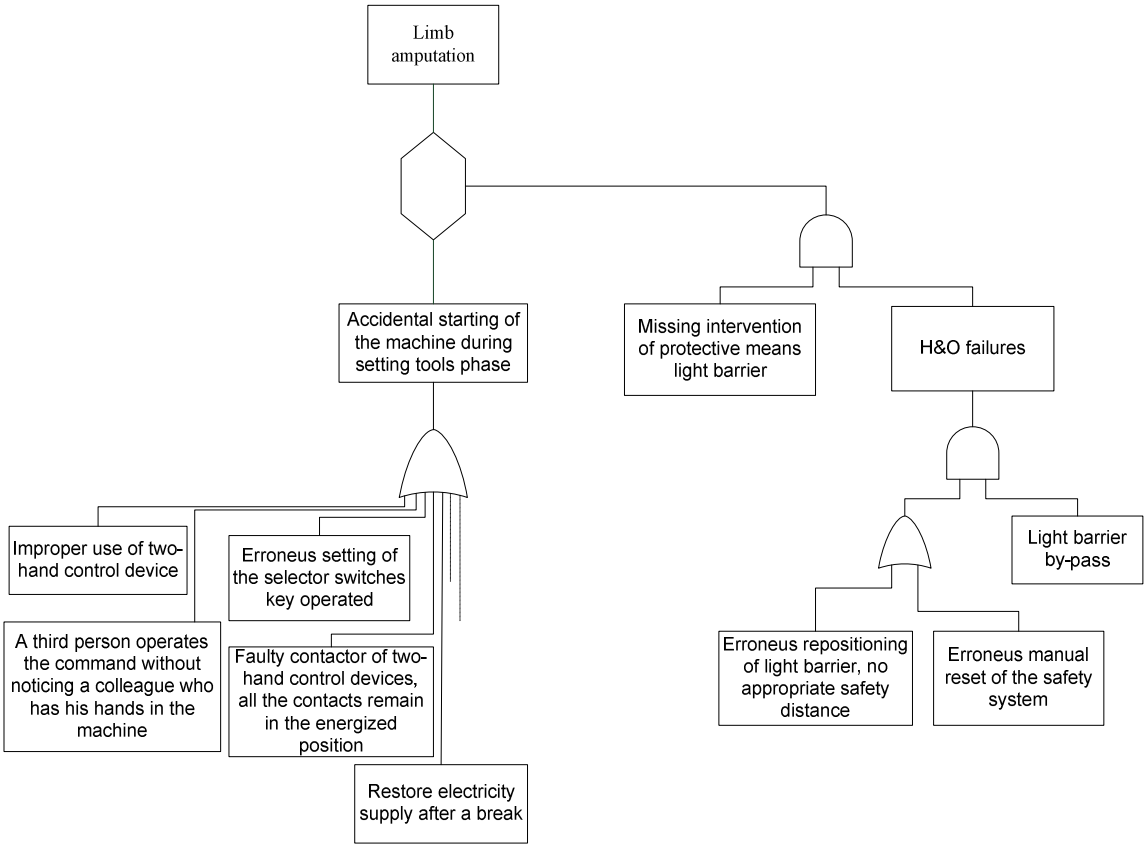


Figure 17: Fault tree from IROA framework

6.2 IDDA APPROACH

IDDA is an Event Tree empowered with conditionings, both logic and probabilistic.

This mean is a computerized version of General Logic, whereas Event Tree remains an important instrument within this Logic. It is a tool aimed to a correct and coherent application of the probability theory.

Through this approach it is possible to model the logic of the systems; system's representation is done delineating all of its possible behaviors which describes the real logic-temporal consequence of the events involved.

Every alternative scenario is developed according to a logical approach Cause – Consequence, by means of a synthetic language, which tends to simulate the human mind.

To apply this methodology is necessary to outline the problem through a semantic-syntactic translation. The instrument for this translation is a logic language that is compound of questions, statements and conditionings.

The aim by Integrated Dynamic Decision Analysis (IDDA) approach is to introduce an analytical methodology which, by examining the structure of the sequence of activities to be done while using the machine is able to identify intrinsic weakness a priory and propose corrective actions to make them safer and more efficient.

This tool should provide effective description of each task performed by operator in sequence in the use of machine , and, above all, highlight the mechanisms which may generate possible operating problems and /or consequences during execution of these tasks.

For a good implementation of logic model a detailed knowledge of human behavior was necessary through once of the different human error analysis techniques.

Starting from the analysis of a technological system through IDDA it is possible to integrate in the logical model a task analysis describing where and why the operator can cheat or by-pass the safety system.

With this model we are expecting a higher SIL called "*operational SIL*" taking into account also human errors bringing to optimised design of the Safety-Related Electrical Control System (SRECS).

6.3 HUMAN RELIABILITY ANALYSIS

Hollnagel (1998) and Kirwan (1994) have listed different human error analysis techniques, including ATHEANA (A Technique for Human Error Analysis), CREAM (Cognitive

Reliability and Error Analysis Method), HEART (Human Error Analysis and Reduction Technique), HEIST (Human Error Identification in System Tools), THERP (Technique for Human Error Rate Prediction) and others.

The goal of these techniques is to determine the reasons for human error occurrence, the factors that influence human performance, and how likely the errors are to occur.

THERP uses the Human Reliability Analysis (HRA) Event Tree (ET) as its basic tool. In Figure 18 the schematic representation of the Human Reliability Event Tree is shown; the capital letter represents the failure while the minuscule letter represents success.

However because THERP is a technique that offers advantages in terms of compatibility with the classical methods related to the reliability there is a great application of the methodology, both fully or as a source of data for evaluation, possibly with other formal methods, of human errors. We have used it for the second purpose.

For these reasons the Technique for Human Error Rate Prediction was chosen to be part of the new methodological approach.

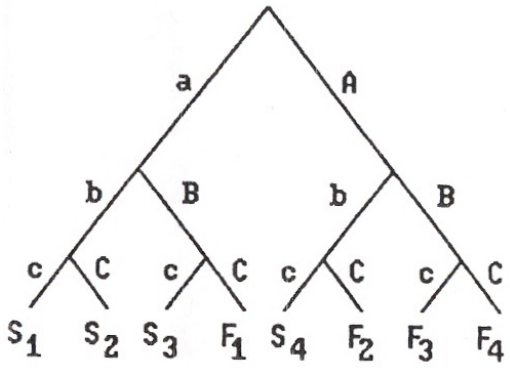


Figure 18: Example of HRA-ET

The scheme below (Figure 19) resumes the dynamics of an accident caused by the human failures.

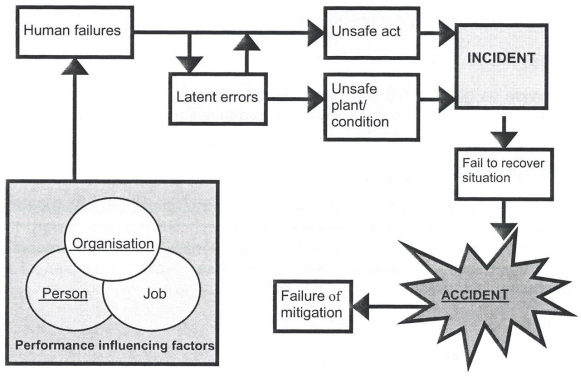


Figure 19: Accidents model

6.4 THERP METHODOLOGY FOR HUMAN AND RELIABILITY ANALYSIS

THERP (Technique for Human Error Rate Prediction) is a method to predict human error probabilities and to evaluate the degradation of a man-machine system likely to be caused by human errors alone or in connection with equipment functioning, operational procedures and practices, or other system and human characteristics that influence system behavior.

THERP requires the analyst to determine whether the error to be examined is one of omission, one of commission, or diagnosis and sources of operator burden include the following:

- time constraints
- diagnosis
- decision making command and control
- physiological factors

Handbook supplies a great number of values of "nominal" probability, groups into 27 tables in the Chapter 20 of the manual [44] in which are contained the data derived from a series of information obtained experimentally and from experts elicitation.

The adjective "nominal" is to indicate that such values don't consider the specific situation and they must therefore be adapted.

The data for human error probability (HEP) in THERP tables referred to the assumption of a lognormal distribution for the human error probability density function (truncated in 0 and 1).

Each type of evaluation of human action is necessarily tied to a certain degree of uncertainty: the introduction of the curves of distribution stems from the need to extend the concept of punctual estimation of probability to human variability.

When the word "Uncertainty Bound" (UCB) is used, we refer it to the extension of Human Error Probabilities (HEPs) related to log-normal distribution (Figure 20). It considers two values: UCB lower and UCB upper; the square root of their division is called Error Factor (EF).

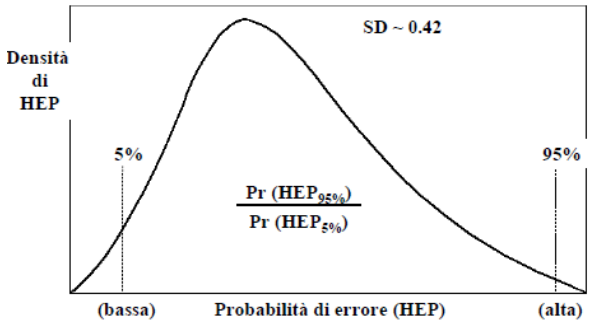


Figure 20: Log-normal distribution

For example in the estimation of HEP with this format: 0.01 (0.003 ÷ 0.03) the UCBS are represented by the numbers in parentheses.

Alternatively, the uncertainty limit value are replaced by the value called Error Factor: the previous case should be indicate as: 0.01 (EF=3), where the EF's value is rounded off.

In this case the limit values can be obtained with the relations:

$UCB_{lower} \cong HEP/EF$

$UCB_{upper} \cong HEP \times EF$

In the tables two values are reported: the median of the distribution and error factor. From this two values the mean value for the lognormal distribution is obtained to be used for assessing the final HEP.

Example value for THERP Table 20-12 (13)

$$X_{50\%} = e^{\mu_z} = 0.003$$

$$EF = X_{95\%} / X_{50\%} = e^{z\sigma_z} = 3$$

$$\mu_z = -5.81$$

$$\sigma_z = \ln 3 / 1.645 = 0.67$$

$$\mu_x = e^{\mu_z + \sigma_z^2/2} = e^{-5.81+(0.67)^2/2} = 3.75 * 10^{-3}$$

Each mean HEP was modified by the effects of stress and experience level in case of emergency conditions, and in the other cases it was changed to take into account the ergonomic constraints (THERP table 20-16).

6.5 TASK ANALYSIS

Task analysis permits to describe the interaction between the operator and the technologies.

To understand when and how the operator could commit mistakes or omitted actions it was necessary to implement a decomposition of operation into component tasks considering the phases of commissioning, normal operations and inspections-maintenance.

The objective of the task analysis is to identify the key tasks so that it could be easier to identify possible wrong action that operator can commit.

For example a task can be mis-applied, operation did not occur, or the operator does more than what the task requires.

In some cases the operator could don't perform as required because he has not enough time.

A good task analysis permits also to avoid that operator has too many tasks, that he doesn't perform two or more step at once, and so on.

In this specific case study the task analysis was performed using an ad hoc template where the machine's functional analysis included the human tasks as well as the technical aspects.

The starting point for a task analysis is a set of clear task descriptors for all the task elements which are associated with particular task. Normally, these descriptions would be derived from a hierarchical task analysis.

6.5.1 Which kind of task analysis?

The purpose of Human Reliability Analysis is to estimate both the likelihood of the human error made in carrying out a required task (commission error) and the human error made when a required action it is not carried out (omission error).

The decomposition approach was a good mean for the purpose to determine the control and information requirements of each step that the operator has to perform with the machinery. This approach was used in the case study of press because decomposition method is the main characteristic of qualitative assessment in THERP.

Task decomposition is an information collection tool which is used to systematically expand upon the basic description of the activities which must be undertaken in each task element.

The starting point for a task decomposition is a set of clear task descriptions for all the task elements which are associated with a particular task, e.g. operational procedure.

This task description must be written at a level of detail which is appropriate for the analyst's purposes.

These information can then be presented for each task element using an appropriate set of sub-headings, so that the total information for each step is decomposed into a series of statements about limited aspects of the task. The sub-heading which are used to decompose the task elements must be specifically selected by the analyst according to the purpose of the particular investigation.

The originator of decomposition methods for task analysis was probably Miller (1953), who suggested that each task element should be decomposed into the following categories: description, subtask, cues initiating action, controls used, typical errors, etc.

However, this categorization does not cover all issues which might be of interest to an analyst, and so in order to address any other issues, it will be necessary to develop other decomposition categories.

6.6 INTEGRATION OF THERP AND TASK ANALYSIS - *CASE STUDY AT TRINITY COLLEGE OF DUBLIN*

A similar case study where a precise task analysis was required, was developed at Trinity College of Dublin (TCD).

High voltage equipment is mostly designed according to technically prescriptive standards, requirements based on electrical engineering safety principles (e.g. CEI IEC 62271-202, High-voltage switchgear and control gear, 2006). However a more risk-based approach to standards and regulation have been advisable to enable designer and user to take an active role in establishing that their installation is inherently safe.

The use of Gas Insulated Switchgear (GIS) for instance is enabling the new substation to be housed indoors and condensed into around one quarter of the space. The manufacturers argue that design improvements in GIS make it virtually "maintenance free" and include: more compact GIS design, higher performance, etc. However some of these improvements have implications for the operators that need to be taken into account. A GIS more compact in fact often means having less space and awkward stations for the technicians during commissioning and maintenance actions. Commissioning, operational checks and inspections and the occasional maintenance interventions are activities during which the technicians need to

interface with the equipment, the issues regarding the interfaces provided have been analysed to identify their relevance in the overall risk assessment of the equipment.

The scope of the present study is to verify trough a risk analysis the impacts that the issues related to deficit in ergonomic design may present for the overall availability and safety of the plant. Issues overlooked by both the technical standards and the designers.

The Risk Assessment was performed using an ad hoc Failure Mode and Effects Analysis (FMEA) template where the functional analysis included the human tasks as well as the technical aspects.

6.6.1 Methodology

The Risk Assessment was performed using an ad hoc Failure Mode and Effects Analysis (FMEA) template where the functional analysis included the human tasks as well as the technical aspects.

Further the Risk levels associated to each possible failure mode was obtained using the risk matrix proposed by the Military Standard MIL-STD-882. The overall method aimed at providing the assessment of a Risk Level similar to the Safety Integrity Level evaluation required by standards descending from IEC 61508 (originally developed for process plants, machineries and vehicles contain requirements and recommendations for validating safety-related electrical, electronic and programmable control systems).

The method would starts with a functional analysis of the equipment to identify all the relevant functions to be performed by the equipment or by an operator with the use of the equipment and the connected failure modes. Some of the failure modes can be determined assessing the Human Errors using the Technique for Human Error Rate Prediction (THERP) developed for the U.S Nuclear Regulatory Commission by Swain and Guttman in 1983.

Information about the order of magnitude of the likelihoods of the events was obtained using equipment reliability data (when available) and THERP for relevant human errors. While the severity was assigned using expert judgment based on the severity classifications guidelines used by the Military Standard MIL-STD-882.

The approach has proved to be flexible and it can be used at different levels of system detail.

Id (1)	Man-machine function (2)	Link – to (3)	Failure-mode (4)	Causes (5)	Consequences (6)	Duration (7)	Times/ Y (8)	Safeguard (9)	L (10)	C (11)	R (12)	Countermeasure (13)

Table 6: Template used for the analysis

The first column identify the man-machine function, column (2) represents each task and sub task performed by the operator that involved a specific components of the GIS.

The objective of column (3) is to consider the direct link between each task, for example in the template annexed to the document at Id 6.4.1 if the gas pressure is right the operator has to proceed with task Id 6.4.3 otherwise he has to refill the gas, Id 6.4.2.

In the column (4) we have considered both the failure mode of the specific component involved in the task both the way making a wrong action of the operator.

Columns (5) and (6) represent respectively the causes of human error and/or failure of device, and the effects of each error and failure mode on main item function.

Columns (7) and (8) are duration of single action/task and how many times per year it is made.

Likelihood (10), severity (11) are the quantitative elements of the analysis necessary to have an estimation of Risk (12).

If presents the safeguard are indicated in column (9) and the last column (13) shows countermeasure to improve safety aspects.

6.6.2 Application

The study consisted of two parts:

- Qualitative analysis
- Quantitative analysis

Only important actions have been modeled.

The most significant issues detected by safety advisor of the company are related to commissioning and inspection/maintenance actions.

For this reason the analysis was focused much more on these aspects, without neglecting the functional part related to normal operation of GIS which is the functional aspect considered by another FMEA performed on the equipment that was used as a benchmark.

Qualitative analysis

In the first part of the analysis the objective was to fill in a detailed manner the first six columns of the template shown above (Table 6) and attached to the document (Annex 12.3).
The phases of the analysis were:
1. Decomposition of operation into component tasks considering the phases of commissioning, normal operations and inspections-maintenance (2)-(3)
2. Identification of the key tasks (2)
3. Identification of the failure modes for each of the component functions considered (4)
4. Detection of causes and consequences of the relevant failure modes (5)-(6)
The content of each boxes of the template was written in a synthetic and understandable form for staff working in the field that was subsequently involved in the quantitative analysis.

Results from qualitative analysis

The study shows that the most significant issues are:
- limited and restrictive working areas; there is insufficient space to work on the installation safely;
- the limited possibilities for applying forces;
- the need for the technicians to work in fixed and awkward posture for sustained periods of time;
- difficulty or complete inability of reading the metrological data;
- slowdown in emergency procedure.

Most of these issues are ergonomics aspects and they have an important relapse on reliability of the whole system and on the wellbeing of the operators.
The bays of the substation are very close to each other and there is not enough space for the operator to access some of the equipment located in between the bays (e.g. it is nearly impossible to perform the gas test on some of the internal bays).

Figure 21: Position of the indicator (above 2mt. high and difficult to read in between bays)

It seems that some basic principles of accessibility were not properly taken into account in the design of the equipment. The lack of basic ergonomics principle in design is reflected in the difficulties encountered by the operators to manually open or close the circuit breakers in case of failure of automatic activation. The risk is that the worker fails to resolve situation in time because he must reach the high position and turn the mechanism shaft in an awkward position and if the operation has to be performed for bays internally located the operator has to walk over the pipelines containing the live cables and the insulating Gas. No platforms were in fact provided to access those areas.

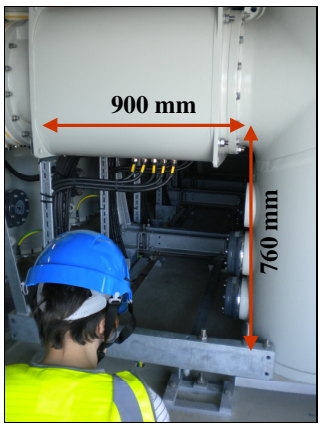


Figure 22: Cables to be reached during commissioning and testing. The picture shows that they are positioned in a confined area accessing which the operator needs to maintain a crawling awkward position**.**

Figure 23: Operator trying to reach while standing on a ladder the manual gear to open the switch in case of failure of the automatic system for the side bay.

The results of the first step of the analysis are confirmed and supported by a survey of users of GIS carried out by the Committee of the Institute of Electrical and Electronics Engineers [34].

The survey highlights once again issues like:

- constricted space for maintenance;

- awkward accessibility of view ports;

- difficulty to read SF_6 gas pressure gauges.

The ergonomic standard ISO 14738:2008 indicates the free space required for different dynamic body postures which may be used during maintenance with moderate force demands, If those indications are compared with some positions and force required in working area of GIS the dimensions seem to be underestimated. This can lead to serious musculoskeletal problems for the operator and could lead the worker to commit a mistake during the relevant commissioning, testing or recovery tasks he or she has to perform.

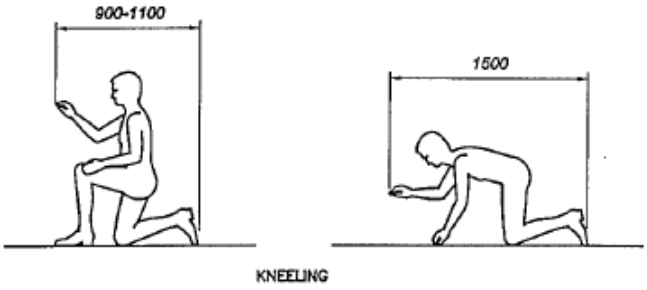


Figure 24: Image taken from the ergonomic standard ISO 14738:2008 showing dimensions for kneeling and crawling positions. Unfortunately the height is not indicated.

Quantitative analysis

Once the qualitative analysis was completed the next step was the semi-quantitative analysis that involved the columns (10) (11) (12) of the template (Table 6).

For the quantification of the hazards in terms of severity of consequences and in terms of probability of occurrence, we have adopted the same approach proposed by the safety standard IEC 62061(Safety of machinery, Functional safety of safety-related electrical, electronic and programmable electronic control systems) with the purpose to follow the guide line used for electric and electronic equipment needed for safety related function as set by the safety integrity level concept proposed by the standard.

To apply the hazard assessment matrix (Table 9) to evaluate if the risk is unacceptable or acceptable it was necessary to verify in what category of likelihood the numerical values, obtained from the quantitative analysis fell and combine it with the judgment on the category of severity for the consequences identified (Table 7 and Table 8 respectively). To make the method more efficient and to justify the choice of range in which likelihood and severity of consequences fall, we have adopted the guide line proposed by the U.S. Military Standard MIL-STD-882.

Hazard severity

Category	Name	Characteristic
I (4)*	Catastrophic	Death Loss of system
II (3)	Critical	Severe injury or mortality Major damage to system
III (2)	Marginal	Minor injury or mortality Minor damage to system
IV (1)	Negligible	No injury or mortality (first aid) No damage to system

*index for safety standard IEC 62061

Table 7: Severity classification

Hazard likelihood

Category	Name	Characteristic	Probability ref. [event/y]
A (5)*	Frequent	Likely to occur frequently Occurred several times in the last 5 years in the company.	$> 10^{-1}$
B (4)	Probable	Will occur several times in life of a component. Has occurred in the company.	10^{-1} to 10^{-3}
C (3)	Occasional	Likely to occur sometimes in life of a component. Has occurred more than once in the industry.	$< 10^{-3}$
D (2)	Remote	Unlikely but possible to occur in life of a component. Has occurred in the industry. No damage to system	$< 10^{-4}$
E (1)	Improbable	Occurrence may not be experienced. Never occurred in the industry	$< 10^{-6}$

*index for safety standard IEC 62061

Table 8: Likelihood classification

Hazard Assessment Matrix and Hazard Risk Index

Frequency of occurrence	Hazard severity			
	I Catastrophic	II Critical	III Marginal	IV Negligible
A - Frequent	IA	IIA	IIIA	IVA
B - Probable	IB	IIB	IIIB	IVB
C - Occasional	IC	IIC	IIIC	IVC
D - Remote	ID	IID	IIID	IVD
E - Improbable	IE	IIE	IIIE	IVE

RI 1	Unacceptable
RI 2	Undesirable (management decision required)
RI 3	Acceptable with review by management
RI4	Acceptable without review

Table 9: Categories used to define the class of risk

The quantitative analysis required to identify the likelihood and consequences related to a variety of events like failure mode of the electrical components, human error, “falls from ladders”, etc. and for this reason these values have been obtained from different sources.

Failure rate of electrical device were provided by reliability data of the manufacturer or through GESCOM data base related to reliability of the components of the Italian electricity grid provided by CESI's report [37]. In this last case the value was not related to each single component but it refers to the whole system; from the MTTF (Mean Time To Failure) it was possible to obtain the respective failure rate using the following relation: $MTTF = 1/\lambda$.

Likelihood of events like "falls from ladders" derives from expert judgment and from records of worker's injury reported by the company involved in the analysis [36].

The failure rate values associated to human error were obtained through the application of THERP model.

THERP (Technique for Human error Rate Prediction) is a method to predict human error probabilities and to evaluate the degradation of a man-machine system likely to be caused by human errors alone or in connection with equipment functioning, operational procedures and practices, or other system and human characteristics that influence system behavior.

THERP requires the analyst to determine whether the error to be examined is one of omission, one of commission, or diagnosis and sources of operator burden include the following:

- time constraints
- diagnosis
- decision making command and control
- physiological factors

The data for human error probability (HEP) in THERP tables referred to the assumption of a lognormal distribution for the human error probability density function (truncated in 0 and 1). In the tables two values are reported: the median of the distribution and error factor. From this two values the mean value for the lognormal distribution is obtained to be used for assessing the final HEP.

Example value for THERP Table 20-12 (13)

$$X_{50\%} = e^{\mu_z} = 0.003$$

$$EF = X_{95\%} / X_{50\%} = e^{z\sigma_z} = 3$$

$$\mu_z = -5.81$$

$$\sigma_z = \ln 3 / 1.645 = 0.67$$

$$\mu_x = e^{\mu_z + \sigma_z^2/2} = e^{-5.81+(0.67)^2/2} = 3.75*10^{-3}$$

Every HEP obtained from the lognormal distribution were reported on the table (Table 10) used for the assessment (The complete table is in the Annex 12.3).

Item n°	Subtask description for HRA-MAN	Mean HEP	Stress level/ergonomic constraints*	Source THERP table	Modified HEP	Total HEP
2.1.1	Operator wrong wiring choosing the wrong cable.	1.12E-02	1	20-12 (13)	1.12E-02	1.12E-02
2.2	Operator cannot see the indicator.	3.75E-03	10	20-10 (1)	3.75E-02	4.37E-02
2.2	Check heater and thermostats are working omitted.	1.25E-03	5	20-7 (3)	6.25E-03	
2.3.1	Visual and physical check if the manual opening and closing of the earth switch is inhibited when the circuit breaker is in a closed position omitted.	1.25E-03	10	20-14 (1)	1.25E-02	1.25E-02

Table 10: Extract of THERP table for subtask 2.1.1, 2.2 and 2.3.1

Each mean HEP was modified by the effects of stress and experience level in case of emergency conditions, and in the other cases it was changed to take into account the ergonomic constraints (THERP table 20-16).

For those ergonomic constraints that completely prevent the job from being effectively carried out it was assigned factor 10, for those constraints that could force the operator to err a multiplication of a factor 5 was used. In some cases it was chosen to use the upper bound level, the 95th percentile HEP of lognormal distribution, to consider the worst case in a conservative manner (e.g. The gas sampling and testing procedures for instance has to be carried out in very adverse conditions where the location of some of the sample points between bays make it nearly impossible for the operator to reach and use them).

The likelihood obtained in the above cases was also discounted to take into account the actual timeframe over which certain tasks are carried out in the life period of the equipment (e.g. commissioning is 1/ 30 years, where 30 years is the expected life duration of the equipment, and Maintenance interventions 1/5 years).

Results from quantitative analysis

The analysis was able to identify two types of consequences:

1) the impact of ergonomic constraints on the operator, and its safety

2) the loss of primary functions of the plant, the loss of efficiency, the possible disruption to customers, etc.

It is important to notice that using the new approach to functional analysis the FMEA was able to take into account more functions and related failure than the ones normally considered for similar equipment.

The hazard risk index for each failure mode fell into two different classes:

One is unacceptable (Risk index 1), this index was usually obtained for cases where the ergonomics constraints made it nearly impossible for the operator to effectively carry out his/her task. The other risk index commonly obtained (Risk Index 2) refers to undesirable situations where the operation is possible but awkward to perform such that the operator may be more easily induced to make mistakes. In those cases the consequences are severe both for the operator safety and for the plant efficiency.

In case of undesirable risk, management decision is required. Annex 1 contains a summary of the results obtained for the risk Assessment of the GIS with all the failure modes leading to a risk index 1 or 2.

The template used for TCD's case study has proved a useful mean and was applied to generate the input file for the logical model in IDDA approach.

7. PROPOSED FINAL APPROACH

There are two crucial aspects related to modelling man-machine interaction in Quantitative Risk Analysis (QRA) context:

1. the need to insert human interaction in the logical model of QRAs techniques;
2. the quantification of effect of human interaction.

The modelling of inappropriate behaviours of human being is the "malfunction" of behaviours of operators.

As happens in general QRA , the analysis related to human-machine interaction in a reliability study are of two types: qualitative and quantitative.

The qualitative analysis is oriented to define the typologies of inappropriate behaviours and to study the systemic and environmental conditions that encouraged and influenced them.

The objective of quantitative analysis is to define the probability of each wrong action and the consequences of accident sequences related to them.

Usually human-machine interactions are represented through logical binary states, success/failure, and human errors are modelled as omitted actions provided by procedures.

Other mode of failure, like inappropriate actions originated by representation errors, wrong reasoning or by misdiagnosis, that produce an intersection of different accident scenarios, are not specifically identified. These inappropriate actions are identified as error of commission and are more and more important in the human factor study in QRA.

To take into account methodology able to include in a formal way human and programmatic errors is essential to develop advanced QRA.

In literature different methodologies of human reliability exist and for this study the most appropriate method was THERP for two reasons: the former because it was effectively applied in the case study of Dublin, the latter because this methodology is strongly linked to data base in which are contained the data derived from a series of information obtained experimentally and from experts elicitation (chapter 6 paragraph 6.6.1).

7.1 COMBINATION OF TASK ANALYSIS, IDDA AND THERP

The proposed model is designed precisely with the aim of transferring the I.D.D.A. philosophy to the in-depth study of the deviations which may occur during human implementation of operational procedures.

To do that it was necessary to identify useful methodology deal with human factors.

The large database based on real data, coupled with the fact that the THERP is strongly oriented to engineering analysis of human errors, led to choose this method.

Once identified the machine's behavior and the possible malfunction in which this can fall, with relatives influence for the operator, it was necessary to develop a detailed analysis of procedure to be performed, identifying all possible operator's error and omission.

A good task analysis was important requirement for the implementation of input file in I.D.D.A. software.

7.1.1 A real example to define e new embedded methodology

The new embedded methodology was applied to the procedure for the use of a press including setting of the equipment, functional check and processing material during normal use of the machine.

For a good and complete task analysis a similar template used in the case study related to Gas Insulated Switchgear was implemented (Table 11 and Annex 12.4).

Id.	Man-Machine function	Link to	Failure mode	Causes	Consequences
1	**Work on the press (only one operator)**		-		
1.1	**Setting of the equipment**	1.1.2	Operation by two instead of one person	Wrong operation mode	Increase probability of injury for the operator
1.1.2	Check area is clear of tools	If clear 1.1.4, if not clear 1.1.3	Omission (operator doesn't check), some operator left some tool in dangerous zone	Omitting a step or important instruction from a formal or ad hoc procedure, lack of concern	Increase probability of injury for the operator

Table 11: Template related to procedure using of Hydraulic press

In this specific case study the failure mode and causes related to the failure are extrapolated, in many cases, from the BGIA study (Chapter 5 paragraph 5.2.1).

7.1.2 Implementation of general model

Once task analysis has been created the second step was to prepare the Input File finalized to run the I.D.D.A. program.

The task analysis related to use of press has been described with I.D.D.A.'s syntax:

1. Identification of the events related to the operation of the system itself and construction of a list of levels, with questions and affirmations, which represents the elementary matter of the logical model and also the nodes in the event tree.
2. Construction of a 'reticulum' indicating the addresses (subsequent level) to be visit after each response in each level, and a comment string that allows the user to read the logical development of a sequence.
3. Association to each of the levels of a probability, which represents the expectation degree of the failure or unwanted event and of an uncertainty ratio, which represents the distribution.
4. Definition of all the constraints, which can modify run time the model, fitting it to the current knowledge status.

8. APPLICATION

Once defined the structure of the new methodology, it was applied to the case study related to the hydraulic press.

The task analysis was implemented on the bases of the operating procedure for the use of the machinery.

The *ad hoc* template was filled evaluating the failure modes for each interaction between man and machinery. These failures could be related to both devices and human error.

After completing the task analysis it was possible to implement the source file to run it with the I.D.D.A. program.

8.1 IMPLEMENTATION OF THE SOURCE FILE

The problem has to be reproduced in the program to aim at developing constituents, and alternative sequences, in a clear, unambiguous and complete way.

The problem has to be represented with a series of questions related to the occurrence or not of the subsequent random events. The questions have to be accompanied by the possible consequences, on the subsequent events, of the response that they receive out of the hypothesis.

Every random event is fully characterised by these fundamental elements:

- Identification number
- Probability assigned to the event
- Two integers. The first represents the number of the random event that follows in the sequence the question in case of success, the second represents the subsequent question in case of failure.

The syntax of file source presents this form:

```
                    :Setting of the equipment number of operators required is one
ID LEVEL            1 0.03 0. 10 145 3 'Num op.' 'one' 'more than one'
                    :Check area is clear of tools
                    10 0.0125 0. 15 150 3 'Op. checks' 'yes' 'no'        DESCRIPTION
                    20 100 0.004 1
                    :Presence of tools in dangerous area
PROBABILITY         15 0.0048 0. 25 20 3 'Area free' 'yes' 'no'
                    :Clean dangerous area
                    20 0.0125 0. 25 150 3 'Op. cleaned' 'yes' 'no'      FOLLOWING ADDRESS
                    20 100 0.004 1
                    :Put press on intermittently command
                    25 0.00133 0. 30 150 3 'Op. correct button' 'yes' 'no‘
                    …
```

What has been written represents the trellis on which to move the logical questions, but it is lacking in both logical and probabilistic conditioning which are necessary for the full definition of the system.

In this case we have used logical conditioning known as of second type and conditional probability of first type.

8.1.1 Syntax of logical conditioning of second type

The need to relate the probability of success or failure of different actions, gives rise to one of the fundamental problems of human reliability analysis is the determination of dependency relationships.

This type of conditioning defined the determination of success or failure of the action referred by the question or of the following logical events in case of success or failure relevant to the previous questions or logic levels.

The syntax is given by a sequence of two integers.

These integers start with 1 or 2 depending on whether the conditioning is caused by the success or failure of the event. The second integer is odd, if the conditioning of the conditioned event is on success and even if it is on failure.

We show the example where if the operator comes into contact with tools and suffers a damage (**2**= “yes, upper limb amputation”), the program must stop with "Operator injured" (**3**= “yes, operator injured”) (Annex 12.5).

```
:Dynamics of injury for the operator
170 0.37 0. 190 190 3 'Upper limb amputation' 'no' 'yes'
14 190 0 0
23 190 0 0
:Injury to the operator
190 1 0. 0 0 3 'Op. injured' 'yes' 'no'
```

8.1.2 SYNTAX OF PROBABILISTIC CONDITIONING OF FIRST TYPE

The need to relate the probability of success or failure of different actions, gives rise to one of the fundamental problems of human reliability analysis is the determination of dependency relationships.

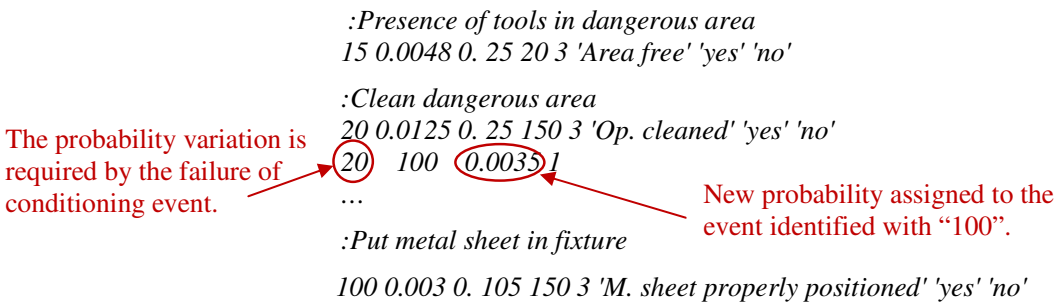
To take into account this concept in the source file, we used the probabilistic conditioning of first type.

The syntax is given by a series of two integers and two real numbers.

The first integer represents the statement that if the conditioning event is on success or failure the conditional probability of a subsequent event has to be changed.

The second integer coincides with number of conditioned event. The real number provides the new probability to assigned to the conditioned event.

We report an example where the operator doesn’t clean the tools area and introduces the raw material to form the metal sheet. In this case it will be more likely that operator suffers injuries or that the metal sheet is not properly positioned.



To fix the new increased value of probability an operational sensible choice was made. We based the choice on statistical data where it was possible. The increase was around 10%.

If it were possible to obtain more precise data it would be quick to change the data within the structure of the source file.

8.2 APPLICATION OF THE PROGRAM FOR THE DETERMINATION OF CONSTITUENTS

The quantitative analysis required to identify the likelihood related to failure mode of different elements like electrical components, human error, implemented in each level of source file; for this reason these values have been obtained from different sources.

Failure rate of electrical device were provided by reliability data of the manufacturer or calculated trough the theory of technical standard EN IEC 62061.

The failure rate values associated to human error were obtained through the application of THERP model.

Item n°	Subtask description for HRA-MAN	Mean HEP	Stress level/ergonomic constraints	Source THERP table	Modified HEP
36	Light barrier intervines (fails)	9.11E-08	1	SRCF	9.11E-08
37	Op. doesn't stop dangerous operation	1.25E-02	1	20-7 (4)	1.25E-0
38	Contact with tools	3.00E-03	1	INAIL	3.00E-03
39	Hurt	1.50E-01	1	INAIL	1.50E-01

Data references extracted from THERP table.

Below we show in which way the value of Human Error Probability of level number 37 was obtained:

$$X_{50\%} = e^{\mu_z} = 0.01$$

$$EF = X_{95\%} / X_{50\%} = e^{z\sigma_z} = 3$$

$$\mu_z = -4.61$$

$$\sigma_z = \ln 3 / 1.645 = 0.67$$

$$\mu_x = e^{\mu_z + \sigma_z^2/2} = e^{-4.61+(0.67)^2/2} = 1.25 * 10^{-2}$$

The source program was played back and we obtained all possible top events and their probability of occurrence.

At this point in order to assign the SIL to the safety function, for example the light barrier, it has been necessary to make a selection and applying certain conditions to extract only the probability of occurrence of injury associated with failure of the barrier or with by-pass of the device.

To do this we applied the IDDA function (SPELSXP) to select the constituents that involve a given top event and in this specific case "Operator injured".

A matrix was built to communicate to the program the conditions to search.

The events that have to be present in the same time must be written in the same row; on the contrary if the elementary events are "in OR", they must be written in a different row.

CONDITIONS (The same ROW=AND the same COLUMN=OR)

Examining the case of light barrier the simultaneous conditions are "Operator injured" and "light barrier not intervenes". The conditions in OR will be the events that explain why the light barrier could not intervene: "Operator omits to recovery safe guards", "Operator doesn't recover safe guards in correct position" or "Operator by-pass the safety device".

At the end the matrix presents a shape of this type:

CONDIZIONI (stessa RIGA = AND stessa COLONNA = OR)

MATRIX

190,P -140,P -65,P
190,P -140,P -67,P
190,P -140,P 107,P

COSTITUENTI ESAMINATI : 3650
*COSTITUENTI SELEZIONATI : **2340***

In this way, 2340 constituents were found. Each probability of these constituents has been calculated and added together to obtain cumulative probability.

This probability can be associated to the probability of dangerous failure expressed in the technical standard.

Once obtained the cumulative probability, it was necessary to translate it into a numerical index to apply the matrix of technical standard EN IEC 62061, thereby carrying out the assignment of the level of integrity required for light barrier.

To justify the choice of the category in which the probability of occurrence of injury falls we have used the guidelines provided by the U.S. Military Standard MIL-STD-882 (Table 12).

We have obtained a probability of occurrence equal to $2.7*10^{-2}$ and we have associated this value to category B.

E L E N C O T O T A L E C U T - S E T S

N. COSTIT. CUT MINIMO ORDINE CUT PROBABILITA' CUMULATA

---

1 0 2 4.352E-03
2 0 2 4.292E-03
3 0 2 2.775E-03
…
2340 1144 11 7.697E-32

PROBABILITA' CUMULATA CUT-SETS **2.718E-02**

Category (Cl)	Name	Characteristic	Probability ref. [event/y]
A (14-15)	Frequent	Likely to occur frequently Occurred several times in the last 5 years in the company.	**> 10^{-1}**
B (11-13)	Probable	Will occur several times in life of a component. Has occurred in the company.	**10^{-1} to 10^{-3}**
C (8-10)	Occasional	Likely to occur sometimes in life of a component. Has occurred more than once in the industry.	**< 10^{-3}**
D (5-7)	Remote	Unlikely but possible to occur in life of a component. Has occurred in the industry. No damage to system	**< 10^{-4}**
E (3-4)	Improbable	Occurrence may not be experienced. Never occurred in the industry	**< 10^{-6}**

Table 12: Classification of probability according to U.S. Military standard

The severity of injuries in case of contact between the operator and tools is critical so that the index will be equal to 4 (Table 13).

Severity	Name	Characteristic
3/4	Critical	Severe injury or mortality Major damage to system
2	Marginal	Minor injury or mortality Minor damage to system
1	Negligible	No injury or mortality (first aid) No damage to system

Table 13: Severity classification

Once identified likelihood and severity of consequences (Table 12 and Table 13), applying the matrix of risk (Table 14) allowed to assign *"Operational SIL"* to the safety function represented by light barrier taking into account the human factors from the beginning of the analysis.

Severity (S_e)	Class (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Table 14: Matrix for the assignment of SIL

From the application of matrix we obtained SIL equal to three for the light barrier. This means that the architecture of the device has to ensure at least the level 3 of availability.

8.3 SIL COMPUTATION FOR LIGHT BARRIER TROUGH THE NEW APPROACH

To verify that the Safety-related Electrical Control System satisfies a Safety Integrity Level equal to three it was built a new source file that takes into account only the light barrier evaluating all the ways it can fail or be by-passed by the operator.

Unlike the source files built in the previous part the objective of analysis is to discover if the device will be available or not when it is called upon to intervene as shown in the level 40 in the source file.

```
:Light barrier
1 0.0000000911 0. 10 40 3 'l.b. works' 'yes' 'no'
24 40 0 0

:Recovery of the safe guards
10 0.000039 0. 20 40 3 'Op. restores the safe guards' 'yes' 'Op. omits'
24 40 0 0

:Recovery of the safe guards in correct position
20 0.000069 0. 30 40 3 'Correct distance transmitter and receiver' 'yes' 'no'
24 40 0 0

:By-pass the device
30 0.00077 0. 40 40 3 'Op.no by-passes device' 'yes' 'no'
13 40 0 0
24 40 0 0

:Availability of light barrier
40 1 0. 0 0 3 'l.b. available' 'yes' 'no'
```

Running the source file we obtained five constituents and also in this case we are interested only in the Top Event: “Light barrier is not available”.

For this reason we applied again the function SPELSXP to select the desired T.E. In this way we obtained four constituents.

```
NOME DEL FILE SORGENTE  : P8lbf.INP
NOME DEL FILE DI OUT    : RIS5lbf.OUT
Livello Iniziale        :   1
NOME FILE PUNTATORI     : RIS5lbf.PUN

TIPO della SELEZIONE    : g
NOME FILE OUTPUT        : RIS8lbfs.PUN
NOME FILE COMPLEMENTARE : RIS8lbfe.PUN

CONDIZIONI (stessa RIGA = AND  stessa  COLONNA = OR)
-40,P    0,    0,    0,    0,    0,0   0,0   0,0   0,0   0,0

COSTITUENTI ESAMINATI   :       5
COSTITUENTI SELEZIONATI :       4
```

It means that in four cases the light barrier fails with a certain probability. The sum of the four probabilities gives the cumulative probability.

At this point it is possible to verify if the cumulative probability falls in the interval of probability related to SIL three; if it is included in that interval it satisfies the requirement previously requested (Table 15).

SIL	PFH
3	$\geq 10^{-9}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 15: Correspondence between SIL and probability of dangerous failure

The following figures shows the selected constituents and then computation of the cumulative probability.

```
EVENTO  ris8lbfs.PUN    della PARTIZIONE  ris8lbf.OUT

    ---------------------------
    COSTITUENTE Numero :     1

 1  l.b. wor yes     +     1.-9.11E-08              1.00E+00
10  Op. rest yes     +     1.-3.90E-05              1.00E+00
20  Correct  yes     +     1.-6.90E-05              1.00E+00
30  Op.no by no      -       7.70E-04               7.70E-04
40  l.b. ava no      - V     1.00E+00               7.70E-04

                          PROBABILITA' uguale a  :  7.70E-04
```

COSTITUENTE Numero : 2

1	*l.b. wor yes*	*+*	*1.-9.11E-08*	*1.00E+00*
10	*Op. rest yes*	*+*	*1.-3.90E-05*	*1.00E+00*
20	*Correct no*	*-*	*6.90E-05*	*6.90E-05*
40	*l.b. ava no*	*- V*	*1.00E+00*	*6.90E-05*

PROBABILITA' uguale a : 6.90E-05

COSTITUENTE Numero : 3

1	*l.b. wor yes*	*+*	*1.-9.11E-08*	*1.00E+00*
10	*Op. rest Op. omit*	*-*	*3.90E-05*	*3.90E-05*
40	*l.b. ava no*	*- V*	*1.00E+00*	*3.90E-05*

PROBABILITA' uguale a : 3.90E-05

COSTITUENTE Numero : 4

1	*l.b. wor no*	*-*	*9.11E-08*	*9.11E-08*
40	*l.b. ava no*	*- V*	*1.00E+00*	*9.11E-08*

PROBABILITA' uguale a : 9.11E-08

E L E N C O T O T A L E C U T - S E T S

N.	COSTIT.	CUT MINIMO	ORDINE CUT	PROBABILITA'	CUMULATA
1	0	1	7.699E-04	87.69E+00	%
2	0	1	6.900E-05	95.55E+00	%
3	0	1	3.900E-05	99.99E+00	%
4	0	1	9.110E-08	10.00E+01	%

PROBABILITA' CUMULATA CUT-SETS 8.780E-04

SIL	PFH
3	$\geq 10^{-9}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

We verified that cumulative probability is $8.78*10^{-4}$ ensuring a Safety Integrity Level lower than that assigned. This highlights the fact that although the architecture of the light barrier was characterised by a high reliability the human factor affects the final result in a very significant way.

9. CONCLUSIONS

The new value calculated with the integrated approach is comparable with the value obtained by mere qualitative risk analysis suggested by the technical standard EN IEC 62061.

Once the value of probability, calculated with the new methodological approach, has been converted in the index of probability, the range in which it falls is the same as the standard method.

It is clear however that the Integrated Dynamic Decision Analysis permits a construction of the problem much more detailed and accurate, allowing to take into consideration also the important aspect related to man-machine interface.

This first important result highlights that taking into account the human factor in the assignment of SIL (*Operational SIL*) is likely to imply the request of a very high level of reliability of the component when it has a very high importance from the point of view of operator's safety. In fact this new methodological approach has great importance when the interaction between human being and machinery is strong, less into the field of large automatic plants.

Furthermore, the probability of dangerous failure (PDF) of the light barrier calculated trough IDDA results significantly higher than the probability linked exclusively to the device architecture. This could mean that the reliability of the architecture of the system was previously overestimated and that probably the design of the light barrier is not sufficient to ensure that the operator does not commit wrong actions.

On the whole, this study shows that more exhaustive evaluation is necessary and that the interface between the operator and the equipment cannot be neglected.

To improve the safety for the operator the best approach will be:

- to have a strong commitment;
- to increase the training of the employee particularly on the job;
- to implement the operational procedure;
- to increase the protection level of intrinsic safety of the electrical devices.

To take into account this conclusions and to comply with the previous analyzed technical standard it is necessary to assess the human factors trough a detailed task analysis. This tool has to describe every elementary action that the operator performs. For each action the analyst identifies the possible error of commission or of omission that the operator is likely to commit.

Once identified the correct sequence of tasks and the likely failure modes, the analyst is able to implement the source file to apply the Integrated Dynamic Decision Analysis (IDDA).

Including particular conditions into the file for the subsequent application (SPELSXP) allows to select the events that involve the safety function that one wants to analyze, as explained during the application in chapter 8. In this way it is possible to obtain a cumulative probability that, when converted into an index of probability, permits to assign the *Operational Safety Integrity Level* to the Safety-related Electrical Control Systems (Table 14, chapter 8).

At this point the last phase will be to verify if the physical safety device applied to the machinery complies with the *Operational SIL* assigned in the previous way using once again the IDDA approach (chapter 8, paragraph 8.3).

If the SIL calculated in the last step corresponds with the one previously assigned, the SRECS will be considered reliable also in case of a hypothetical wrong behavior of the operator and the goal will be reached. Otherwise it will be necessary to carry out a failure reduction analysis and to repeat the analysis.

To have a correct methodological approach to take into account human factors is useful also to have evidence where a safety device could fail. It is difficult for engineers to change human nature and therefore, it is indispensable to try to remove opportunities for error by changing the work situation: so it is possible to change the plant or equipment design or the method of working. Alternatively, it is possible to mitigate the consequences of error or provide opportunities for recovery.

It is important to remind that safety analysis should interest all people involved, not only engineers, but also all those who work in, as designers, users and producers.

10. SYMBOLS AND NOTATIONS

APM:	Automatic Protective Means
CCF:	Common Cause Failure
CPC:	Common Performance Condition
CTA:	Cognitive Task Analysis
DRV:	Driver
EF:	Error Factor
EFC:	Error Forcing Context
EI:	Erroneous Intervention
EIPM:	Erroneous Intervention Protective Means
EPC:	Error Producing Condition
ESF:	Engineered Safety Features
ET:	Event Tree
FMEA:	Failure Modes & Effects Analysis
FO:	Field Operator
FT:	Fault Tree
HAZOP:	Hazard and Operability
HEP:	Human Error Probability
HF:	Human Factors
HFE:	Human Failure Event
HFI:	Human Failure Identification
H&OF:	Human and Organisational Factors
HRA:	Human Reliability Analysis
HRA-ET	Human Reliability Analysis Event Tree
HTA:	Hierarchical Task Analysis
INH:	Inhibit
IROA:	Integrated Recursive Operability Analysis
IDDA	Integrated Dynamic Decision Analysis
MI:	Missing Intervention
MMI:	Man Machine Interaction
MPM:	Manual Protective Mean
OAT:	Operator Action Tree
P&ID:	Piping and Instrumentation Diagram
PRA:	Probability Risk Assessment
PSFs:	Performing Shaping Factors
RHOA:	Recursive Human Operability Analysis
ROA:	Recursive Operability Analysis
SAD	Strategy-Action-Diagnosis
SLI	Success Likelihood Index
SRK:	Skill Rule Knowledge

TA:	Task Analysis
TDO:	Technical Department Operator
TE:	Top Event

11. REFERENCES

[1]. CEI EN 62061:2005-04, Sicurezza del macchinario - sicurezza funzionale dei sistemi di commando e controllo elettrici, elettronici ed elettronici programmabili correlate alla sicurezza.

[2]. T. Barnet, K.T. Kosmowski & M. Sliwinski, Determing and verifying the safety integrity level of the control and protection systems under uncertainty, Gdansk University of Technology, Poland.

[3]. F. Brissaud & D. Charpentier, Safety instrumented system reliability evaluation with influencing factors, Instituit National de l'Environment Industriel et des Risques (INERIS) – DCE, Verneuil-en-Halatte, France.

[4]. Yves Langeron, Anne Barros, Antoine Grall & Christophe Berenguer, On combination of Safety Integrity Levels (SILs) according to IEC61508 merging rules, – Universitè de Technologie de Troyes/ICD, CNRS, Troyes, France.

[5]. UNI EN ISO 14121-1, Sicurezza del macchinario - Valutazione del rischio, Parte 1: Principi.

[6]. [UNI EN ISO 12100-1, Sicurezza del macchinario - Concetti fondamentali, principi generali di progettazione" Parte 1: Terminologia di base, metodologia.

[7]. Linee guida ISPESL, Caratteristiche di funzionalità e sicurezza dei dispositivi a protezione del fronte lavorativo delle presse piegatrici idrauliche.

[8]. ISO/TR 14121-2:2007, Sicurezza delle macchine - Analisi dei rischi.

[9]. UNI EN 12622:2003, Sicurezza delle macchine utensili – Presse piegatrici idrauliche.

[10]. Martin Schonbecka,b, Marvin Rausanda, Jan Rouvroyeb, Human and organizational factors in the operational phase of safety instrumented systems: A new approach, a Department of Production and Quality Engineering, Norwegian University of Science and Technology, Norway; b Department of Technology Management, Eindhoven University of Technology, The Netherlands, 2009.

[11]. James Reason, Human error: models and management, Department of Psychology, University of Manchester, 2000.

[12]. UNI EN 693:2009, Machine tools-Safety-Hydraulic presses.

[13]. UNI EN ISO 13849-1:2008, Sicurezza del macchinario Parti dei sistemi di commando legate alla sicurezza, Parte 1: Principi generali per la progettazione.

[14]. Safety of machinery -Safety-related parts of control systems - Part 1: General principles for design.

[15]. Ulisse Belladonna, Elementi di Oleodinamica - Hoepli- edizione 2008.

[16]. Igor Bazovsky, Reliability Theory and Practice, Prentice-Hall, edizione 1996.

[17]. P.Clerici, A. Guercio, N. Todaro, Il fattore umano: tecniche di analisi, soluzioni, e prospettive.

[18]. V. Rumawas & B.E. Asbjornslett, A proposed model to account human factors in safety-critical,Norwegian University of Science and Technology (NTNU), Trondheim, Norway, ESREL 2010.

[19]. E. Hollnagel, Cognitive Reliability and Error Analysis Method (CREAM), Elsevier, edizione 1998.

[20]. CEI EN 62079:2002-01, Preparazione di istruzioni - Struttura, contenuto e presentazione.

[21]. UNI 10893:2000, Documentazione tecnica di prodotto. Istruzioni per l'uso. Articolazione e ordine espositivo del contenuto.

[22]. D. Embrey, Task Analysis Techniques, Human Reliability Associates Ltd., 2000.

[23]. P.Trucco, M.C. Leva, A probabilistic cognitive simulator for HRA studies (PROCOS), Elsevier Science, 2006.

[24]. N. McDonald, S. Corrigan, C. Daly, S. Cromie, Safety management systems and safety culture in aircraft maintenance organizations, Pergamon Safety Science 34 (2000) 151-176, 2000.

[25]. B. Kirwan, Human error identification techniques for risk assessment of high risk systems, Elsevier Science, 1998.

[26]. M.C. Leva, F. Mattei, A. Kay, S. Cromie, M. De Ambroggi, T. Kontogiannis, The Development of a method and a tool for dynamic task representation as part of a virtual reality application, EU research project VIRTHUALIS.

[27]. M.C. Kim, P. H. Seong, E. Hollnagel, A probabilistic approach for determing the control mode in CREAM, Reliability Engineering & System Safety 91 pp. 191-199, 2006.

[28]. J. Annett, Neville A. Stanton, Task Analysis, Taylor Francis, 2000

[29]. Human Engineering, MIL-ST_1472 Department of defence design criteria standard.

[30]. D. German, H. Blackman, Human Reliability & Safety Analysis Data Handbook, John Wiley & Sons, 1994.

[31]. B. Kirwan, L. Ainsworth, A guide to task analysis, Taylor & Francis, 1992.

[32]. CEI IEC 62271-202, High-voltage switchgear and control gear, 2006.

[33]. NUREG 0700, Human system interface design review guidelines, 2002.

[34]. IEEE, Gas insulated substation experience feedback, IEE/PES Substation Committee, 2010.

[35]. D. Swain, H.E. Guttmann, NUREGCR 1278F, Handbook of human reliability analysis with emphasis on nuclear power plant application (final report), 1983.

[36]. Injury statistics of ESB staff, 2009

[37]. Report CESI, Development of processing tools with a limited but significant data, 2005.

[38]. Buakaew S. Reliability Centered Maintenance For Gas Insulated Switchgear Maintenance Conference Proceedings CEPSI 2010 Taipei on October 24-28, 2010.

[39]. Terna, Technical specifications- Prefabricated equipment with isolated metal closure with gas SF6 for ratings equal or higher than 140 kV, 2010.

[40]. M. Demichela, N. Piccinini, Integrated dynamic decision analysis (IDDA) a new approach for risk analysis, AIDIC Conference Series, Vol. 6,93-100,2003.

[41]. N. Piccinini, M. Demichela , Risk based decision-making in plant design,Canadian Journal of Chemical Engineering, pp. 7, , Vol. 86, 2008.

[42]. M. Demichela, N. Piccinini, Integrated Dynamic Decision Analysis (IDDA): an Advanced Tool for Risk Analysis, PSAM 7, International Conference on Probabilistic Safety Assessment and Management, 2004.

[43]. M. Demichela, R. Galvagni, N. Piccinini, PSA in dynamic process system through integrated dynamic decision analysis, In: CISAP2 "2nd International Conference on Safety & Environment in Process Industry", AIDIC (ITA), Naples 21- 24 May 2006, pagine da 43 a 48, 2006.

[44]. A. D. Swain, H. E. Guttmann, NUREG/CR 1278F, Handbook of human reliability analysis with emphasis on nuclear power plant applications, Final Report.

12. ANNEX

12.1 ANNEX: HAZID TEPMLATE

N°	Fasi	Pericolo Deviazione	Cause	Conseguenze	F			D	R
					P_r	Av	F_r		
1.	Montaggio/Sollevamento								
1.1	Aggancio pressa ai quattro attacchi	Mancato aggancio	Dimenticanza dell'operatore OR Nodi realizzati in modo scorretto	Nessuna conseguenza pericolosa per la salute e sicurezza del lavoratore	2	1	1	1	4
1.2	Sollevamento della pressa per appoggiarla su travi di legno	Caduta dall'alto	Errato ancoraggio Utilizzo sistema di sollevamento con portata inferiore al peso della macchina	Traumi dovuti a schiacciamento	3	1	1	2	10
1.3	Messa in bolla della pressa	Scorretto livellamento della macchina per errato settaggio delle viti di livellamento	Errore dell'operatore Rottura di una o più viti di livellamento Superficie di appoggio non uniforme	Perdita di efficienza della macchina se inclinata.	1	1	1	1	3
2.	Installazione								
2.1	Allacciamento elettrico								
2.1.1	Collegamento interruttore generale con un cavo tripolare + terra	Contatto diretto con elementi in tensione Contatto indiretto con elementi che entrano in tensione in condizioni di guasto.	Contatto con la massa sotto tensione (massa va a terra)	Folgorazione	3	1	1	4	20
2.1.2	Messa a terra fissando all'apposito morsetto una corda nuda posto nelle vicinanze dell'interruttore generale	Contatto indiretto con elementi che entrano in tensione in condizioni di guasto.	La massa va in tensione	Folgorazione	3	1	1	4	20
2.1.3	Collegamento cavi elettrici dei pulsanti e dei dispositivi di protezione elettrica come da progetto e schemi allegati	Cortocircuito	Contatto indebito tra i conduttori	I dispositivi di protezione non intervengono	3	1	1	3	15
2.2	Allacciamento acqua per sistema di raffreddamento								
2.2.1	Installazione sistema di raffreddamento	Mancato allacciamento	Errore operatore	Mancato raffreddamento con surriscaldamento dei circuiti idraulici e della macchina	2	1	1	1	4
2.3	Riempimento serbatoio olio idraulico								
2.3.1	Apertura serbatoio per controllarne il grado di pulizia	Contatto con olio	Errore dell'operatore	Irritazione della pelle	3	1	2	2	12
2.3.2	Chiusura serbatoio	Errata chiusura del serbatoio	Errore dell'operatore	Funzionamento degradato della macchina OR	3	1	1	1	5

N°	Fasi	Pericolo Deviazione	Cause	Conseguenze	F			D	R
					P_r	Av	F_r		
				La macchina non parte					
2.3.3	Riempimento serbatoio a serbatoio chiuso attraverso il bocchettone di carico posizionato sul coperchio del serbatoio	Rovesciamento di olio idraulico OR Riempimento con olio non idoneo	Errore dell'operatore Errore dell'operatore	Formazione di chiazze d'olio sul pavimento e rischio scivolamento Introduzione nel circuito oleodinamico di corpi estranei accidentalmente contenuti nell'olio OR Rottura della macchina	3	1	2	2	12
2.3.4	Lubrificazione guide scorrimento del piano mobile della pressa	Gocciolamento olio idraulico	Errore operatore	Formazione di chiazze d'olio sul pavimento e rischio scivolamento	4	1	1	1	6
3.	**Messa in funzione/Avviamento**								
3.1	Controllo corrispondenza collegamenti elettrici fatti con il progetto	Collegamenti di versi da quelli indicai nel progetto	Errore installatore	La macchina non parte OR Azionamento comandi incontrollato	2	1	1	1	4
3.2	Accensione macchina	Mancata accensione della macchina	Mancanza E.E. OR Collegamenti elettrici non corretti	La macchina non si avvia, mancata produzione	2	1	1	1	4
4.	**Funzionamento/Ciclo di lavorazione**								
4.1	**Messa a punto degli utensili**								
4.1.1	Posizionamento dello stampo idoneo al tipo di lavorazione da eseguire	Contatto con utensile	Avviamento intempestivo della macchina	Ferita, schiacciamento, cesoiamento, amputazione arti superiori	3	3	4	4	40
			Caduta per gravità della trave che trattiene il punzone per un guasto del sistema idraulico, per un guasto meccanico o per un guasto del sistema di controllo elettrico	Ferita, schiacciamento, cesoiamento, amputazione arti superiori	3	1	4	4	32
4.1.2	Posizionamento sullo stampo della dima di centraggio	Contatto con utensile (punzone)	Avviamento intempestivo della macchina	Ferita, schiacciamento, cesoiamento, amputazione arti superiori	3	1	4	3	24
			Caduta per gravità della trave che trattiene il punzone per un guasto del sistema idraulico, per un guasto meccanico o per un guasto del sistema di controllo elettrico	Ferita, schiacciamento, cesoiamento, amputazione arti superiori	3	1	4	3	24
4.2.	**Alimentazione e caricamento materie prime**								

N°	Fasi	Pericolo Deviazione	Cause	Conseguenze	F			D	R
					P_r	Av	F_r		
4.2.1	Inserimento pezzo di acciaio da lavorare (manuale)	Contatto con utensile (punzone)	Avviamento intempestivo della macchina causa errata posizione del contatto di sicurezza	Ferita, schiacciamento, cesoiamento, amputazione arti superiori	3	3	5	4	44
4.3	**Lavorazione materiale (produzione)**								
4.3.1	Selezione del ciclo di lavoro con regolazione o verifica dei parametri funzionali della macchina	Errato settaggio del ciclo di lavoro	Errore operatore	Potenziali situazioni di pericolo es. proiezione di materiale verso l'operatore	2	1	5	2	16
4.3.2	Azionamento dispositivo di doppio comando ad azione mantenuta (oss. Non è più ammesso per la produzione UNI EN 12622:2003, solo per fasi di setting come la messa a punto degli utensili, corse di prova, manutenzione e lubrificazione)	Avviamento accidentale	Guasto contattore, tutti i contatti rimangono in posizione eccitata quando la bobina è diseccitata. OR Errore operatore OR una terza persona aziona il comando senza di accorgersi del collega che ha le mani nella macchina	Ferita, schiacciamento, cesoiamento, amputazione arti superiori	3	3	5	4	44
4.3.2.1	Esecuzione del ciclo di produzione	Caduta per gravità accidentale della trave durante la produzione	Guasto del sistema idraulico Guasto meccanico Guasto del sistema comando elettrico	Lesioni arti superiori	2	1	5	3	24
4.3.2.2	Muting	Contatto con gli strumenti	Guasto del circuito oleodinamico	Lesioni arti superiori	3	3	4	3	30
4.3.3	Disattivazione macchina a fine ciclo	Mancato funzionamento del fine corsa elettrico	Guasto del dispositivo di fine corsa per mancata apertura dei contatti	Schiacciamento arti superiori	4	1	5	3	30
5.	Servizi								
5.1	Energia elettrica	Mancanza energia elettrica	Interruzione dalla rete	Arresto improvviso della macchina	3	1	5	1	9
5.2	Acqua per sistema di raffreddamento	Mancanza acqua OR Raffreddamento insufficiente	Mancanza acqua da rete OR Mancato funzionamento dello scambiatore calore causa tubi dell'acqua incrostati OR Mancato collegamento a rete idrica	Surriscaldamento della macchina	1	1	1	1	3
6.	**Sistemi protettivi**								
6.1	Doppi pulsanti di discesa con dispositivo di simultaneità congiuntamente ad una bassa velocità di chiusura	Contatto indebito/cortocircuito OR Guasto attuatore	Avviamento accidentale della macchina	Ferita, schiacciamento, cesoiamento, amputazione dita e mani	3	1	5	4	36

N°	Fasi	Pericolo Deviazione	Cause	Conseguenze	F			D	R
					P_r	Av	F_r		
6.2	Barra di protezione con dispositivo di sicurezza elettro-pneumatico	Mancato intervento della barra di protezione	Guasto del dispositivo di sicurezza	Mancata interruzione della discesa del piano mobile della pressa	3	1	5	2	18
6.3	Pulsante di emergenza pressa, fungo rosso	Mancato funzionamento del dispositivo di protezione	Guasto del dispositivo di comando OR Mancato ripristino manuale delle condizioni di sicurezza a seguito di precedente intervento del dispositivo	Mancata interruzione del ciclo di lavorazione	3	3	5	4	44
6.4	Pulsante di emergenza posto sul quadro elettrico	Mancato funzionamento del dispositivo di protezione	Guasto elettrico, mancata apertura dei contatti	Mancata interruzione del ciclo di lavorazione	3	1	2	2	12
6.5	Piano mobile munito di micro di sicurezza elettrico che ferma il movimento quando si raggiunge la quota minima di mm.200	Mancato arresto del piano mobile in fase di discesa	Guasto del micro di sicurezza	Potenziale situazione di pericolo in caso di presenza dell'operatore Il pezzo in lavorazione viene rovinato	3	1	1	4	20
6.6	Pressostati	Aumento di pressione nei circuiti idraulici della pressa	Malfunzionamento pressostato per mancata chiusura dei contatti	Collasso delle tubazioni Proiezione di fluido caldo e pericolo di scottature Incendio	4	3	5	2	24
6.7	Valvole di sicurezza Valvole di sovrappressione	Aumento della pressione nei circuiti idraulici della pressa	Mancato intervento delle valvole di sicurezza	Collasso delle tubazioni Proiezione di fluido caldo e pericolo di scottature Incendio	2	3	4	2	18
6.8	Funzioni di sicurezza del sistema di controllo: - Funzione di arresto legata alla sicurezza avviata da un mezzo di protezione - funzione di ripristino manuale - funzione di riavviamento - funzione di inibizione - funzione di azione mantenuta - prevenzione dell'avviamento inatteso - modalità di comando e selezione di modalità - interazione tra le diverse parti dei sistemi di comando legate alla sicurezza - funzione di arresto di emergenza	Mancata messa in sicurezza della macchina	Avaria del sistema di controllo	Ferita, schiacciamento, cesoiamento, amputazione dita e mani	2	3	4	3	27

N°	Fasi	Pericolo Deviazione	Cause	Conseguenze	F			D	R
					P_r	Av	F_r		
7.	**Manutenzione**								
7.1	Pulizia della pressa								
7.1.1	Accesso all'area di pericolo della pressa	La macchina riparte senza autorizzazione	Guasto elettrico al sistema di comando OR Guasto del software OR Influenza esterna sul sistema elettrico (campo elettromagnetico indotto)	Frattura agli arti Cesoiamento	3	1	3	3	21
7.1.2	Inserimento blocco meccanico di sicurezza della slitta della pressa	Mancato inserimento del blocco meccanico di sicurezza della slitta della pressa	Errore dell'operatore OR Caduta per gravità della trave che trattiene il punzone per un guasto del sistema idraulico, per un guasto meccanico o per un guasto del sistema di controllo elettrico	Accesso pericoloso alla macchina	3	1	3	3	21
7.1.3	Inserimento della sicurezza meccanica con selettore a chiave	Mancato inserimento della sicurezza	Guasto del selettore OR Errore dell'operatore	Accesso pericoloso alla macchina	3	1	3	3	21
7.1.4	Apertura dell'interruttore generale di alimentazione elettrica della pressa	Mancata interruzione dell'alimentazione elettrica	Guasto elettrico OR Dimenticanza dell'operatore	Contatto diretto e folgorazione	2	1	3	4	24
7.1.5	Chiusura delle saracinesche	Saracinesche bloccate aperte	Perdita d'olio pericolosa OR Svuotamento del serbatoio	Formazione di chiazze d'olio sul pavimento e rischio scivolamento	3	1	3	2	14
7.2	Controllo funzione delle spie luminose di sicurezza	Mancato controllo delle spie luminose	Errore operativo	Mancato intervento del dispositivo di protezione su chiamata e situazione di pericolo per l'operatore	2	1	5	2	16
7.3	Pulizia del fluido idraulico	Fuoriuscita di fluido	Fluido in pressione	Schizzi d'olio, ustione	2	1	3	2	12
7.4	Controllo mensile del serraggio delle viti	Mancato serraggio delle viti	Errore operativo	Funzionamento fuori specifica della macchina Fermi macchina indesiderati	3	1	3	1	7
7.5	Pulizia annuale del serbatoio	Mancata pulizia del serbatoio	Errore operativo	Funzionamento degradato della macchina Fermi macchina indesiderati	2	1	2	1	5
7.5.1	Sostituzione della cartuccia filtri	Mancata sostituzione della cartuccia filtri	Errore operativo	Intasamento circuiti e degrado della macchina Fermi macchina indesiderati	2	1	3	1	6

N°	Fasi	Pericolo Deviazione	Cause	Conseguenze	F			D	R
					P_r	Av	F_r		
7.6	Controllo giornaliero dei pulsanti di emergenza	Mancato controllo dei pulsanti di emergenza	Errore operativo OR Errata procedura	Mancato intervento del dispositivo di protezione su chiamata.	2	1	5	1	8
7.7	Controllo giornaliero delle barre di sicurezza	Mancato controllo delle barre di sicurezza OR Il dispositivo non viene ripristinato correttamente dopo il controllo	Errore operativo Errore operativo	Accesso pericoloso alla macchina	2	1	5	1	8
7.8	Controllo sistema idraulico								
7.8.1	Controllo settimanale dei giunti per tubi	Fuoriuscita di fluido ad alta pressione	Rottura casuale della tubazione OR Cadute di pressione OR Errore dell'operatore	Schizzi di fluido sul manutentore e irritazione cutanea	2	1	4	2	14
7.8.2	Controllo settimanale flange	Perdita dalle flange Fuoriuscita di fluido ad alta pressione	Rottura casuale della tubazione OR Errore dell'operatore nel serraggio delle viti	Schizzi di fluido sul manutentore e irritazione cutanea	2	1	4	2	14
7.8.2.1	Cambio guarnizioni	Fuoriuscita olio idraulico	Mancata chiusura delle saracinesche	Formazione di chiazze d'olio sul pavimento e rischio scivolamento	3	1	2	1	6
7.8.3	Controllo mensile tubi flessibili di pressione								
7.8.3.1	Verifica tubi flessibili di pressione	Fuoriuscita di fluido ad alta pressione	Rottura casuale della tubazione OR Caduta di pressione OR Errore dell'operatore per mancata chiusura delle saracinesche	Schizzi di fluido sul manutentore e irritazione cutanea	2	1	3	2	12
7.8.4	Controllo mensile tubi flessibili di scarico	Fuoriuscita di fluido ad alta pressione	Rottura casuale della tubazione OR Errore dell'operatore per mancata chiusura delle saracinesche	Schizzi di fluido sul manutentore e irritazione cutanea	2	1	3	2	12
7.8.5	Controllo mensile della taratura delle valvole di massima pressione	Mancata taratura delle valvole	Errore operativo	Pericoloso aumento di pressione nel circuito oleodinamico Perdita di efficienza della macchina	2	1	3	1	6
7.8.6	Controllo mensile della taratura delle valvole di	Mancato controllo periodico delle valvole di	Errore operativo	Malfunzionamento valvole con pericoloso	2	1	3	1	6

N°	Fasi	Pericolo Deviazione	Cause	Conseguenze	F			D	R
					P_r	Av	F_r		
	sicurezza	sicurezza		aumento di pressione nel circuito oleodinamico Perdita di efficienza della macchina					
7.8.7	Controllo mensile pressostati	Perdite di olio pericolose	Mancata chiusura delle saracinesche	Formazione di chiazze d'olio sul pavimento e rischio scivolamento Svuotamento del serbatoio	3	1	3	1	7
7.9	Controllo annuale del sistema elettrico								
7.9.1	Lavori su sistema elettrico	Contatto diretto con elementi sotto tensione	Mancanza di protezioni contro i contatti diretti OR Mancata apertura interruttore generale di alimentazione elettrica della pressa.	Folgorazione	3	1	2	4	24
7.9.2	Lavori su sistema elettrico	Contatto indiretto	Mancanza di protezioni contro i contatti indiretti OR Guasto messa a terra	Folgorazione	2	1	2	4	20
7.10	Lubrificazione settimanale	Mancata lubrificazione	Errore operativo	Intasamento circuiti idraulici Perdita di rendimento della macchina	2	1	4	1	7
7.11	Riparazione								
7.11.1	Operazione di cambio punzone	Avviamento intempestivo della macchina	Cortocircuito OR Errore dell'operatore	Traumi dovuti a schiacciamento	3	1	1	3	15
		Caduta punzone	Errore dell'operatore	Traumi dovuti a schiacciamento	2	1	1	3	12
7.11.2	Operazione di cambio della matrice	Avviamento intempestivo della macchina	Cortocircuito OR Errore dell'operatore	Traumi dovuti a schiacciamento	3	1	1	3	15
7.11.3	Riposizionamento della zona protetta	Mancato riposizionamento della protezione	Errore/dimenticanza dell'operatore	Traumi dovuti a schiacciamento	4	1	1	3	18
7.11.4	Sostituzione guarnizioni cilindro imbutitura	Mancata sostituzione Utilizzo di una guarnizione non idonea	Errore operativo Errore operativo	Perdita di efficienza della macchina Fermo macchina indesiderato	3	1	2	1	6
7.11.5	Sostituzione guarnizioni valvola di riempimento DN 120	Mancata sostituzione Utilizzo di una guarnizione non idonea	Errore operativo Errore operativo	Perdita di efficienza della macchina Fermo macchina indesiderato	3	1	2	1	6
7.11.6	Sostituzione guarnizioni cilindro premilamiera	Mancata sostituzione	Errore operativo	Perdita di efficienza della macchina	3	1	2	1	6

N°	Fasi	Pericolo Deviazione	Cause	Conseguenze	F			D	R
					P_r	Av	F_r		
		Utilizzo di una guarnizione non idonea	Errore operativo	Fermo macchina indesiderato					
7.11.7	Sostituzione guarnizioni sicurezza meccanica	Mancata sostituzione Utilizzo di una guarnizione non idonea	Errore operativo Errore operativo	Perdita di efficienza della macchina Fermo macchina indesiderato	3	1	2	1	6
7.11.8	Sostituzione guarnizioni estrattore pneumatico	Mancata sostituzione Utilizzo di una guarnizione non idonea	Errore operativo Errore operativo	Perdita di efficienza della macchina Fermo macchina indesiderato	3	1	2	1	6
8.	**Messa fuori servizio**								
8.1	Scollegamento macchina da rete elettrica	Mancato scollegamento macchina da rete elettrica	Errore operativo	Avviamento intempestivo della macchina	2	1	1	1	4
8.2	Indicazione con opportuna segnaletica di messa fuori servizio della macchina	Mancata segnalazione	Errore operativo	Potenziale utilizzo pericoloso della macchina	3	1	1	1	5
8.3	**Smantellamento**								
8.3.1	Smontaggio macchina	Caduta pezzi	Errore operativo	Schiacciamento	2	1	1	2	8
8.3.2	Sollevamento	Caduta pezzi dall'alto	Errore operativo	Schiacciamento	3	1	1	2	10
8.3.3	Imballaggio								
8.4	**Smaltimento differenziato**								
8.4.1	Recupero oli	Mancato recupero olio idraulico	Errore operativo	Perdita di olio e sversamento con creazione di pozze d'olio sul pavimento Esposizione al rischio chimico dell'operatore	2	1	1	2	8
8.4.2	Recupero parti metalliche	Mancato recupero parti metalliche	Errore operativo	Mancata applicazione della raccolta differenziata	2	1	1	1	4
8.4.3	Recupero RAEE	Mancato recupero rifiuti apparecchiature elettriche ed elettroniche	Errore operativo	Mancata applicazione della raccolta differenziata	2	1	1	1	4
8.4.4	Recupero materiale plastico	Mancato recupero e stoccaggio di materiale plastico	Errore operativo	Mancata applicazione della raccolta differenziata	2	1	1	1	4

12.2 ANNEX: APPENDIX OF HAZID ANALYSIS AND RISK ASSESSMENT

N°	Phases	Hazard Deviation	Cause	Consequences	(Cl)			(S_e)	R
					P_r	A_v	F_r		
2.	**Installation**								
2.1	Connection								
2.1.1	Cable connection of switch	Direct contact OR Indirect contact with elements that come voltage under fault conditions.	Contact with the ground voltage	Electrocution	3	1	1	4	20
4.	**Processing cycle**								
4.1	**Setting tools**								
4.1.1	Positioning the die suitable to the type of work involved	Contact with tool	Accidental start of the machine	Hurt, crushing, cutting, upper limb amputation	3	3	4	4	40
			Gravity fall of the slide/ram because of a failure of hydraulic system, fault of hydraulic system	Hurt, crushing, cutting, upper limb amputation	3	1	4	4	32
4.2.	**Feeding and loading raw materials**								
4.2.1	Feeding of metal sheet (by hand)	Contact with tool	Accidental start of the machine because of wrong position of the safety contact.	Hurt, crushing, cutting, upper limb amputation	3	3	5	4	44
4.3	**Material processing**								
…	…	…	…	…	…	…	…	…	…

12.3 ANNEX: TABLE USED FOR THE RISK ASSESSMENT OF THE GIS

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
2	**Commissioning**						
2.1	**Check the conformity of the wiring with the diagrams**						
2.1.1	Commissioner checks wiring and equipment functional checks	Commissioner makes an error in choosing the wrong circuit /cable	Awkward reachability of wiring in the back, ladder needed, wrong labelling	Short-circuit/Secondary equipment damage	C	II	2
		Commissioner falls from the ladder	Awkward reachability of wiring in the back, ladder needed	Injury			
		Commissioner gets caught with his fingers	Door does not remain open (fingers trapped)	Injury			
			Handle designed to open front panel causes risk of trapping fingers.				
2.2	**Operator check heater and thermostats are working (to keep humidity low within cabinet)**	Commissioner falls from the ladder	Working at height (on ladder)	Injury	B	II	1
		Commissioner can not see the thermostat indicator	Awkward reachability	Moisture ingress			
				Deterioration of internal contacts			
		Heater fault	Heater is broken	Moisture ingress			
				Deterioration of internal contacts			
		Check omitted	Awkward reachability	Moisture ingress			
				Deterioration of internal relay contacts			

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
2.3	**Check interlocks are properly working**						
2.3.1	Visual and physical check if the manual opening and closing of the earth switch is inhibited when the circuit breaker is in a closed position.	Check ommitted	Operator cannot see the position of the circuit breaker in the middle bays.	Failure of interlocking allowing the earth swithch to be closed on to a live busbar.Short-circuit to earth.Falls from height.	C	II	2
2.4	**Commissioning of HV cables (checking of phasing and checking of cables integrity)**	Operator misinterprets the correct position of cables	Tagging not clear or not readable, tagging of bays not readable from bottom positions where cables are	Incorrect phasing.Cable fault to earth			
		Commissioner is bent in awkward position and increases likelyhood of making a mistake	Cables are in very awkward positon in the bays that are not on the outside, difficult to reach and difficult to keep working in that positions (how long do they need for each bay to connect cable in that position?)	Musculoskeletal Injuries	C	II	2
2.4.1	Commissioning of the CT circuits.	Commissioner misinterprets the identity of CT cores and secondary cable locations. Position increases the likelyhood of making a mistake.	CT cores are in very awkward positon in the bays that are not on the outside, difficult to reach and difficult to keep working in that positions (how long do they need for each bay to test the cables?)	Testing of incorrect bay.Testing of incorrect CT core.Musculoskeletal injuries	C	III	2

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
2.5	**Fill SF6 gas in bays**	Refill not properly performed	Difficult to reach certain refill valves in bays not on the outside (feasbility of building a passegeway between circuit breaker and earth switch section currently there are cables that could be position underneath the passegeway)	Low gas pressure.Circuit breaker lock out.Falls from a height.Musculosketal Injuries.	B	II	1
		Refil omitted	Difficult to reach certain refill valves in bays not on the outside (feasbility of building a passegeway between circuit breaker and earth switch section currently there are cables that could be position underneath the passegeway)	Low gas pressure.Circuit breaker lock out.Falls from a height.Musculosketal Injuries.			
2.6	**Measurement of gas quality**						
2.6.1	Check gas at right pressure	Visual check failed	Manometers are not readable (facing the wrong side (see picture) and in positions not easy to reach or see.	Low gas pressure.Circuit breaker lock out.Musculoskeletal Injuries.	B	II	1
		Misinterpret the gas pressure (can not see gauge)	Manometers are not readable (facing the wrong side (see picture) and in positions not easy to reach or see.	Low gas pressure.Circuit breaker lock out.Musculoskeletal Injuries.			

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
		Commissioner falls from height	Manometers are in positions not easy to reach or see and operator is forced to use a ladder.	Injuries			
		Manometers fault	Manometer is broken	Low gas pressure.Circuit breaker lock out.			
2.6.2	Check dew point for moisture content.Check % SF6.	Misinterpret the dew point and moisture content (commission)	Inaccessible gas testing points	SF6 gas Integrity.Insulation breakdown.Musculoskeletal Injuries.	B	II	1
		Commissioner falls from height	Inaccessible gas testing points	Injuries			
2.6.3	Check for gas leaks	Gas leak	Incorrect mounting of flange/pressure release valve failure	Release of toxic substance.Release of greenhouse gas.	C	II	2
		Insulation integrity unknown (omission)	Inaccessible gas testing points	Insulation breakdown.Musculoskeletal Injuries.			
2.7	**Inspection of Circuit Breaker** (N.1and 2 in the figure**)**						
2.7.1	Check circuit breaker operation	Circuit breaker fails to open on 'open' command.Circuit breaker fails to close on 'close command.	Incorrect control wiring.Incorrect local operation.	Incorrect operation.	D	III	3
2.7.2	Check circuit breaker timing	Omission (commissioner does not check)	Awkward reachability	Protection may operate incorrectly.	C	III	2
2.7.3	Check circuit breaker position indication	Circuit breaker in wrong position	Cannot view position indication	Interlocking should prevent Operator attempting to operate a disconnect on load.	D	III	3

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
2.7.4	Check circuit breaker contact resistance	Omission (commissioner does not check)	Awkward reachability	Awkward reachability.Effect on circuit breaker performance.	B	III	2
		Falls from height		Injury			
2.8	**Test Voltage Transformer** (N.6 in the figure)						
2.8.1	Check if the equipment is adequately earthed	Omission (commissioner does not check)	Unsafe location /awkward position	Short circuit to earth	B	II I	2
		Commissioner wrong to detect the position of indicator	Unsafe location /awkward position	Short circuit to earth			
2.8.2	Check if supporting metal-work is earthed	Omission (commissioner does not check)	Difficult tocheck the earthing arrangement for the internal bays.	If frame is not earthed the frame could be come live in case of fault (risk of being elelctrocuted)	B	I	1
2.8.3	Check if the main earth strap on the secondary side is easily accessible without causing interference to the VT secondary winding	Omission (commissioner does not carry out visual check or electrical test)	Awkward reachability / access.	VT not earthed.Electrical test not carried out.	C	II I	2
2.8.4	Perform Omicron Ratio Test	Omisison to check VT ratio	VT secondary cores are in a very awkward positon situated on top of the bay.Difficult to reach and difficult to keep working in that positions for a long duration.	Possible faulty condition may result in malfunctioning of the Relay (might not trip in event of fault)	C	II I	2
2.8.5	Check insulation resistance between windings (Primary to secondary)	Inaccessible to test	Unsafe location /awkward position	Short circuit to earth	C	II	2

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
2.8.6	Check insulation resistance between windings and earth	Inaccessible to test	Unsafe location /awkward position	Short circuit to earth	C	II	2
2.8.7	Check insulation resistance of secondary circuits to earth	Inaccessible to test	Unsafe location /awkward position	Short circuit to earth	C	II	2
2.8.8	Check if the continuity of windings is correct	Inaccessible to test	Unsafe location /awkward position	Short circuit to earth	C	II	2
2.8.9	Check if the Primary Winding earth is adequately protected	Inaccessible to carry out visual check	Unsafe location /awkward position	Broken earth.Open circuit.	C	III	2
2.8.10	Check if the secondary wiring is used appriopriate to the application	Inaccessible nameplate to gather information/inaccessible to test	Unsafe location /awkward position	Protection & metering windings get mixed up.Incorrect operation of protection.	C	II	2
2.8.11	Check earthing on secondary terminals	Inaccessible to check	Unsafe location /awkward position	Protection & metering windings get mixed up.Incorrect operation of protection.	C	II	2
2.8.12	Check if phasing is correct to terminals and relays	Crossing of phases	Problems with labelling	Protection & metering windings get mixed up.Incorrect operation of protection.	C	II	2
2.8.13	Check if the ratio of the VT is correct	Omisison to check VT ratio	VT secondary cores are in a very awkward positon situated on top of the bay.Difficult to reach and difficult to keep working in that positions for a long duration.	Possible faulty codnition may result in malfunctioning of the Relay (might not trip in event of fault)	C	II	2
2.8.14	Check VT winding application for metering and protection	Inaccessible to check	Awkward reachability / access.	Protection & metering windings get mixed up.Incorrect operation of protection.	C	II	2
2.8.15	Verify if VT secondary wiring connections have been checked for tightness	Loose connection	Connections removed during tests	Arcing of contacts.Electrocution.Equipment does not operate	B	II	2

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
			No adequate training				
2.8.16	Record VT data and test results	Commissioner does not record the test results	Asset data is inaccessible in the internal bays	Insufficient asset data and test results for the equipment.	C	II I	2
2.9	**Test Current Trasformer** (N.5 in the figure)						
2.9.1	Check if supporting metal-work is earthed	Omission (commissioner does not check)	Difficult to check the earthing arangement on internal bays bays.	If frame is not earthed the frame could be come live in case of fault (risk of being elelctrocuted)	B	I	1
2.9.2	Check if the equipment is earthed correctly	Omission (commissioner does not check CT secondary circuits.)	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	If frame is not earthed the frame could become live in case of fault (risk of being elelctrocuted)	B	II I	2
2.9.3	Check if the equipment is firmly bolted down	Omission (commissioner does not check)	Difficult to access holding dowm bolts on internal bays	Vibrations could displace equipment.	C	II I	2
2.9.4	Test insulation resistance	Omission (commissioner does not check)	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	Possible internal fault in CT could go undetected resulting in undetected.Result in HV fault / fire.	C	II	2

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
2.9.5	Perform Omicron Tan Delta Test	Omisison to check condition of insulation	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	Possible undetected faulty insulation condition may result in insulation breakdown	C	II	2
2.9.6	Perform Omicron Ratio Test Results	Omisison to check CT ratio	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	Posisble faulty condition may result in malfunctioning of the Relay (might not trip in event of fault)	C	II	2
2.9.7	Perform CT Analsyer Test	Omisison to check CT ratio	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	Posisble faulty codnition may result in malfunctioning of the Relay (might not trip in event of fault)	C	II	2
2.9.8	Check if a magnetising curve have been conducted on each winding (to check if the correct secondary winding has been connected)	Omission (commissioner does not check)	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	Secondary windings to be used for measuring could be worngly used for protection purposes	C	II	2
2.9.9	Perform a CT Burden Measurement	Secondary current for CT exceeded	Selection of incorrect secondary winding due to location	Protection may operate incorrectly	D	II	2
2.9.10	Check polarity of CT	Omission (commissioner does not check)	CT inacessible to check polarity in middle bays	Protection may operate incorrectly.Polarity of CT incorrect.	C	II	2
2.9.11	Check if unused secondaries are shorted and earthed (Specify which windings & location)	Open circuited CT secondary winding.Induced voltage at	CT inacessible to check if unused secondary cores	Electrocution/Burns	D	I	2

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
		secondary terminals.	are short circuited.				
2.9.12	Check if the HV connections are tightened to the correct torque setting.	Loose connection.	HV connections inaccessible to check torque	Arcing / short-circuit	C	II	2
2.9.13	Record CT data and test results	Commissioner does not record the test results	Asset data is inaccessible in the internal bays	Insufficient asset data and test results for the equipment.	C	III	2
3	**Closure circuit in Normal operation**	Fail close circuit	Main contact damage		C	III	2
			Contact corrosion		C	III	2
			Contact erosion		C	III	2
			Spring mechanism broken"closing spring unwound"		C	III	2
4	**Opening circuit in normal operation**	Fail open circuit	Main contact damage				
			Contact welding together				
			Spring mechanism broken"closing spring wound"				
4.1	**Arc extinction**	Release of substance from the decomposition gas	Leak of enclosure	Exposure to dangerous substances			
		Failure of insulation under electric stress	Disruptive discharge	Electric shock of the operator			

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
5	**Emeregency Opening**						
5.1	**Interrupt fault during fault condition**						
5.1.1	Operator manually opening the breaker in case of fault	Operator fails to resolve situation in time	Very difficult to reach the manual gear to open the switch in case of fault manually especially for the bays in middle positions.		B	II	1
6	**Visual inspections**						
6.1	**Take counter reading if cycles above 10.000 perform minor maintenance**	Operating cycle counter does not work	Operating linkage is loose or defective operating cycle counter is defective	Incorrect maintenance	B	III	2
		Operator can not see the counter	Awkward reachability	Incorrect maintenance			
6.2	**Circuit breaker and motor wound mechanism**						
6.2.1	Inspect cabinet(free of damages), check heater functions, verify ventilation opening allow free air movement, examine view windows must be clear of dust and moisture	Operator fail to make the checks	The window to be checked and the ventilation opening are not easily reacheable	Presence of moisture in the breaker can go undetected	B	II	1
6.3	**Earth Switch -Check position indication and verify that is it the same as the remote position**	Operator fails to detect position indication is incorrect	Distraction	Earth switch may not function correclty.No earths applied for maintenace.	B	II	1
				Lack of earthing during maintenance			
6.4	**Insulations gas and density supervision**						
6.4.1	Check gas at right pressure?	Visual check failed	Manometers are not readable (facing the wrong side (see picture) and in positions not easy to reach or	Low gas pressure.Circuit breaker lock out.	B	II	1

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
			see.				
		Misinterpret the gas pressure (can not see gauge)	Manometers are not readable (facing the wrong side (see picture) and in positions not easy to reach or see.	Low gas pressure.Circuit breaker lock out.			
		Manometers fault	Manometer is broken	Low gas pressure.Circuit breaker lock out.			
6.4.2	Refilling of Gas	Incomplete operation	Inaccessible gas testing points, and manometers not visible	Arc might not be exstinguished as it should, human operator falls form hight	B	II	1
		Refill omitted	Inaccessible gas testing points, and manometers not visible	Arc might not be exstinguished as it should, human operator falls form hight			
6.4.3	Check dew point for moisture content	Misinterpret the dew point and moisture content (commission)	Inaccessible gas testing points	Insulation breakdown	B	II	1
		Operator fall from height	Inaccessible gas testing points.	Injuries			
6.4.4	Check for gas leaks	Gas leak	Incorrect mounting of flange/pressure release valve failure	Release of toxic substance	C	II	2
		Insulation integrity unknown (omission)	Inaccessible gas testing points.	Insulation breakdown. Musculoskeletal injuries			
7	**Minor inspections intervention**						
7.1	**Disconnect from high voltage network**						

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
7.1.1	Disconnection of Equipment	Error in identifying correct bay for disconnection.Labelling	Discrepency in the layout of equipement and standard layout	Hazard of electrocution	B	I	1
		The apparatus is connected to other source of supply	Operator mis-reads the status of the apparatus	Hazard of electrocution			
7.1.2	Apply Hold Off (HO)notes to the point of disconnection	Operator ommission	Operator omitted to apply HO to apparatus due to awkward position	Hazard of electrocution.Falls from height.	B	I	1
7.2	**Earth switchgear on both sides with the earthing switches provided**						
7.2.1	Proof of application of main earth	Error in identifying correct bay to apply main earth.Labelling	Discrepency in the layout of equipement and standard layout	Hazard of electrocution	B	I	1
7.3	**Minor Inspection Circuit Breaker in service**						
7.3.1	Take counter reading if cycles above 10.000 perform minor maintenance	Operating cycle counter does not work	Operating linkage is loose or defective, operating cycle counter is defective	Incorrect maintenance	B	II I	2
		Operator can not see the counter	Awkward reachability	Incorrect maintenance			
7.3.2	Check circuit breaker operation	Circuit breaker spurios opening/reclosing	Circuitr breaker control circuit fault	Incorrect operation	C	II I	2
7.3.3	Check circuit breaker timing	Omission (operator does not check)	Awkward reachability	Protection delay or not correct protection	B	II I	2
7.3.4	Check circuit breaker position indication	Circuit breaker in wrong position	Cannot view position indication	Operation of disconnect on load	B	II I	2
7.3.5	Check circuit breaker contact resistance	Omission (operator does not check)	Awkward reachability	Falls from height. Awkward reachability	B	II I	2

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
7.3.6	Check of motor-wound spring operating mechanisms	Circuit breaker mechanism fails to operate.	Mechanical fault in the mechanism causing spring failure or mechanism failure.	Impact injuries.Eye injuries from flying parts of the mechanism.	C	II	2
7.4	**Minor Inspection Voltage Transformer**						
7.4.1	Check if the equipment is adequately earthed	Omission (operator does not check)	Unsafe location /awkward position	Short circuit to earth.Earth fault.	B	II I	2
		Commission operator wrong to detect the position of indicator	Unsafe location /awkward position	Short circuit to earth			
7.4.2	Check if supporting metal-work is earthed	Omission (operator does not check)	Difficult tocheck the earthing arrangement for the internal bays.	If frame is not earthed the frame could be come live in case of fault (risk of being elelctrocuted)	B	I	1
7.4.3	Check if the main earth strap on the secondary side is easily accessible without causing interference to the VT secondary winding	Omission (operator does not carry out visual check)	Awkward reachability / access.	VT not earthed. Electrical test not carried out	B	II I	2
7.4.4	Perform Omicron Ratio Test	Omisison to check CT ratio	VT secondary cores are in a very awkward positon situated on top of the bay.Difficult to reach and difficult to keep working in that positions for a long duration.	Posisble faulty codnition may result in malfunctioning of the Relay 9might not trip in event of fault)	B	II I	2
7.4.5	Check Insulation resistance between windings (Primary to secondary)	Inaccessible to test	Unsafe location /awkward position	Short circuit to earth	B	II	1
7.4.6	Check insulation resistance between windings and earth	Inaccessible to test	Unsafe location /awkward position	Short circuit to earth	B	II	1
7.4.7	Check Insulation resistance of secondary circuits to earth	Inaccessible to test	Unsafe location /awkward position	Short circuit to earth	B	II	1

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
7.4.8	Check if the continuity of windings is correct	Inaccessible to test	Unsafe location /awkward position	Short circuit to earth	B	II	1
7.4.9	Check if the Primary Winding earth is adequately protected	Inaccessible to carry out visual check	Unsafe location /awkward position	Broken earth.Open circuit.	B	III	1
7.4.10	Check if the secondary wiring is used appriopriate to the application	Inaccessible nameplate to gather information/inaccessible to test	Unsafe location /awkward position	Protection & metering windings get mixed up.Incorrect operation of protection.	B	II	1
7.4.11	Check earthing on secondary terminals	Inaccessible to check	Unsafe location /awkward position	Protection & metering windings get mixed up.Incorrect operation of protection.	B	II	1
7.4.12	Check if phasing is correct to terminals and relays	Crossing of Phases	Problems with labelling	Protection & metering windings get mixed up.Incorrect operation of protection.	B	II	1
7.4.13	Check if the ratio of the VT is correct	Omisison to check VT ratio	VT secondary cores are in a very awkward positon situated on top of the bay.Difficult to reach and difficult to keep working in that positions for a long duration.	Posisble faulty codnition may result in malfunctioning of the Relay (might not trip in event of fault)	B	II	1
7.4.14	Check VT winding application for metering and protection	Inaccessible to check	Awkward reachability / access.	Protection & metering windings get mixed up.Incorrect operation of protection.	B	II	1
7.4.15	Verify if VT secondary wiring connections have been checked for tightness	Loose connection	Connections removed during tests.	Arcing of contacts.Electrocution.Equipment does not operate.	B	II	1
7.4.16	Record VT data and test results	Commissioner does not record the test results	Asset data is inaccessible in the internal bays	Insufficient asset data and test results for the equipment.	B	III	2
7.5	**Minor Inspection Current Trasformer**						

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
7.5.1	Check if supporting metal-work is earthed	Omission (operator does not check)	Difficult to check the earthing arangement on internal bays bays.	If frame is not earthed the frame could be come live in case of fault (risk of being elelctrocuted)	B	I	1
7.5.2	Check if the equipment is earthed correctly	Omission (operator does not check CT secondary circuit)	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	If frame is not earthed the frame could be come live in case of fault (risk of being elelctrocuted)	B	II I	2
7.5.3	Check if the equipment is firmly bolted down	Omission (operator does not check)	Difficult to access holding dowm bolts on internal bays	Vibrations could displace equipment	B	II I	2
7.5.4	Test insulation resistance	Omission (operator does not check)	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	Possible internal fault in CT could go undetected resulting in undetected.Result in HV fault / fire.	B	II	1
7.5.5	Perform Omicron Tan Delta Test (ratio to resistive current to capacitive current)	Omisison to check condition of insulation	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	Possible undetected faulty insulation condition may result in insulation breakdown	B	II	1

id	Man-Machine function	Failure mode	Causes	Consequences	L	C	R
7.5.6	Perform Omicron Ratio Test Results	Omisison to check CT ratio	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	Posisble faulty codnition may result in malfunctioning of the Relay 9might not trip in event of fault)	B	II	1
7.5.7	Perform CT Analsyer Test	Omisison to check CT ratio	CT secondary cores are situated are in very awkward positon. .Difficult to reach and difficult to work in this position for a long duration of time.	Posisble faulty codnition may result in malfunctioning of the Relay 9might not trip in event of fault)	B	II	1
7.5.8	Check if a magnetising curve have been conducted on each winding (to check if the correct secondary winding has been connected)	Omission (operator does not check)	CT secondary cores are situated are in very awkward position. .Difficult to reach and difficult to work in this position for a long duration of time.	Secondary windings to be used for measuring could be worngly used fro protection pupuses	B	II	1
7.5.9	Perform a CT Burden Measurement	Secondary current for CT exceeded	Selection of incorrect secondary winding due to location	Protection may operate incorrectly	C	II	2
7.5.10	Check polarity of CT	Omission (operator does not check)	CT inacessible to check polarity in middle bays	Protection may operate incorrectly.Polarity of CT incorrect.	B	II	1
7.5.11	Check if unused secondaries are shorted and earthed (Specify which windings & location)	Open circuited CT secondary winding. Induced voltage at secondary terminals.	CT inaccessible to check if unused secondary cores are short circuited.	Electrocution/Burns	C	I	1
7.5.12	Check if the HV connections are tightened to the correct torque setting.	Loose connection.	HV connections inaccessible to check torque	Arcing / short-circuit	B	II	1
7.5.13	Record CT data and test results	Commissioner does not record the test results	Asset data is inaccessible in the internal bays	Insufficient asset data and test results for the equipment.	B	III	2

12.4 ANNEX: TABLE USED FOR TASK ANALYSIS OF USE OF A PRESS

ID	Man-Machine function	Link to	Failure mode	Causes	Consequences
1	**Work on the press (only one operator)**		-		
1.1	**Setting of the equipment**	1.1.2	Operation by two instead of one person	Wrong operation mode	Increase probability of injury for the operator
1.1.2	Check area is clear of tools	If clear 1.1.4, if not clear 1.1.3	Omission (operator doesn't check), some operator left some tool in dangerous zone	Omitting a step or important instruction from a formal or ad hoc procedure, lack of concern	Increase probability of injury for the operator
1.1.3	Remove every tools from dangerous area	1.1.4	Omission (operator doesn't remove tools)	Omitting a step or important instruction from a formal or ad hoc procedure, lack of concern	Increase probability of injury for the operator
1.1.4	Put press on intermittently command	1.1.5	Operator presses incorrect button	Error of the operator	Hurt, crushing, cutting, upper limb amputation
			Accidental start of the machine	Wrong wiring of cables, switch shorted out, controls improperly installed	Contact with tools, hurt, crushing, cutting, upper limb amputation
				Defective switch	
				Improperly Maintained	
1.1.5	Unplug and move from the area of operation controlling mobile equipment and any guards there exist	1.1.6	Omission (operator doesn't check)	Omitting a step or important instruction from a formal or ad hoc procedure.	Machine could start accidentally. Hurt, crushing, cutting, upper limb amputation
			Power outage	Operator error, power not locked out	Electrocution/Burns
1.1.6	Closing the mold by pressing the intermittently button	1.1.7	Operator does not use the intermittently button	Operator error	Contact with tools,hurt, crushing, cutting, upper limb amputation
			Accidental start of the machine	Defective button	
1.1.7	Attach the mechanical safety of the slide of the press	1.1.8	Omission (operator doesn't include mechanical lock)	Omitting a step or important instruction from a formal or ad hoc procedure	Increase probability of injury for the operator
				No devices provided	
1.1.8	Enter security mechanical lock with key selector	1.1.9	Operator wrongs to turn the key	The devices permits to turn in the opposite site	Machine is not in safe
			Key selector failure	Contact problem	
1.1.9	Unlock the upper and lower mold halves with appropriate tools	1.1.10	Gravity fall of the mold	Operator doesn't use correct tools, screws loosened	Crushing arms
1.1.10	Lift the stick of time required to run a smooth introduction and removal of mold pressing the intermittently button	1.1.11	Operator presses incorrect button	Operator error, problems with labelling	Contact with tools and crushing arms
1.1.11	Unplug the main motor of the press	1.1.12	Omission (operator doesn't disconnect the machine from electricity)	Operator error, power not locked out	Collision
1.1.12	Remove the mold from the table using the means provided for this purpose	1.1.12.1	Gravity fall of the mold	Operator doesn't use correct tools	
1.1.12.1	The driver of the vehicle used in the operation of lifting and transport must ensure that no one is in dangerous zone	yes 1.1.14; no exit	The driver doesn't see the third operator	Operator error, he has not enough visibility	Collision
1.1.14	Place the new mold on the table, position it with suitable tools		Gravity fall of the mold	Operator doesn't use correct tools	Crushing arms

ID	Man-Machine function	Link to	Failure mode	Causes	Consequences
1.1.14.1	The driver of the vehicle used in the operation of lifting and transport must ensure that no one is in danger zone		The driver doesn't see the third operator	Operator error	Collision
1.1.15	Lock the two mold halves, in definitive way only the top one, adjust the stroke of the bat		Gravity fall of the mold	Fault lock	Contact with tools and crushing arms, amputation, hand injury
			Circumvention of the protection system	The operator by pass the safe guards	Increase probability of injury for the operator
			Omission (operator forgets to lock the two molds)	Omitting a step or important instruction from a formal or ad hoc procedure.	Increase probability of injury for the operator
1.1.16	Recovery of the shelter		Omission (operator forgets to recovery the safe guards)	Omitting a step or important instruction from a formal or ad hoc procedure.	Increase probability of injury for the operator
			Incorrect setting of the operating distance between the transmitter and receiver	Commissioning error of the operator	
			Incorrect setting of the safety distance between the barrier and the danger zone	Commissioning error of the operator	
1.2	**Functional check of the machine - test run**				
1.2.1	Check operating selector – single stroke		Omission (operator doesn't check the selector	Omitting a step or important instruction from a formal or ad hoc procedure	Machine is not under control
1.2.2	Test controls – anti repeat		Omission (operator doesn't test anti-repeat control)	Omitting a step or important instruction from a formal or ad hoc procedure	Machine is not under control
1.2.3	Test controls – protection from accidental activation		Omission (operator doesn't test condition of protection from accidental activation)	Omitting a step or important instruction from a formal or ad hoc procedure	Machine is not under control
1.2.4	Test stop control		Omission (operator doesn't test stop control)	Omitting a step or important instruction from a formal or ad hoc procedure	Machine is not under control
1.2.5	Test good condition of perimeter protection		Omission (operator doesn't test perimeter protection)	Omitting a step or important instruction from a formal or ad hoc procedure	Machine is not under control
1.2.5.1	Check that the guards are securely fastened in place with devices requiring a tool to release them and that no access is possible from any direction to the danger zone		Omission (operator doesn't check if no access is possible to the danger zone)	Omitting a step or important instruction from a formal or ad hoc procedure	
1.2.6	Verify the absence of others in the vicinity of the press		Omission (operator doesn't verify)	Omitting a step or important instruction from a formal or ad hoc procedure	Machine is not under control
1.2.7	Test 2-hand controls - trial stroke with all safe guards in place		Omission (operator doesn't test 2-hand controls)	Omitting a step or important instruction from a formal or ad hoc procedure	Machine is not under control
1.2.8	Record data and test results		Operator does not record the test results	Omitting a step or important instruction from a formal or ad hoc procedure, daily inspection card is not close to the press	Machine is not under control

ID	Man-Machine function	Link to	Failure mode	Causes	Consequences
1.3	**Processing material**				
1.3.1	Put metal sheet in fixture		Metal sheet lowers the level of protection if not properly positioned	Reflection of light of safe barriers creates a by-pass	Safe guards doesn't reveal the presence of hand
1.3.2	Simultaneous pressure and kept up launchers to run the process		Operator by-passes the device	Operator error, simplification of the work, time gain, bad ergonomics, ignorance of risk	Increase probability of injury for the operator
			At the moment of release of one actuator the command start again in an accidental way	Wrong wiring of cables, no interrupt output signal to the release of one or both of the actuators	Contact with tools, hurt, crushing, cutting, upper limb amputation
1.3.3	If the light barrier intervenes, proceed to the manual reset		Omission (operator doesn't reset)	Unsafe location /awkward position	Increase probability of injury for the operator
			Accidental restart of the machine	The reset command is not separated from the start command of the press	Contact with tools, hurt, crushing, cutting, upper limb amputation
1.3.4	Remove formed part		Accidental restart of the machine	Wrong wiring of cables, no interrupt output signal to the release of one or both of the actuators	Contact with tools, hurt, crushing, cutting, upper limb amputation
			Operator doesn't put in safe the machine	Omitting a step or important instruction from a formal or ad hoc procedure	Increase probability of injury for the operator
1.3.5	Place part in bin on floor		Operator doesn't place formed part in correct container	Omitting a step or important instruction from a formal or ad hoc procedure	Some pieces don't reach the quality control
1.3.6	Collect waste processing with special mean and put them in media collection		Omission (operator doesn't clean dangerous area)	Omitting a step or important instruction from a formal or ad hoc procedure	Waste accumulation in the mould
			Operator doesn't use correct tool	Omitting a step or important instruction from a formal or ad hoc procedure	Increase probability of injury for the operator
1.3.7	The operator has to disconnect the power supply if use of hands cannot be avoided		Omission (operator uses hands without disconnecting the power supply	Omitting an important instruction from a formal or ad hoc procedure	Increase probability of electrocution for the operator

12.5 ANNEX: I.D.D.A. FILES

12.5.1 File Source for SIL assignment

```
:Setting of the equipment number of operators required is one
1 0.03 0. 10 145 3 'Num op.' 'one' 'more than one'

:Check area is clear of tools
10 0. 0. 15 25 3 'Op. checks' 'yes' 'no'
20 100 0.004 1

:Presence of tools in dangerous area
15 0. 0. 25 20 3 'Area free' 'yes' 'no'

:Clean dangerous area
20 0.0125 0. 25 25 3 'Op. cleaned' 'yes' 'no'
20 100 0.004 1

:Put press on intermittently command
25 0.00133 0. 30 150 3 'Op. correct button' 'yes' 'no'

:Accidental start of the machine
30 0.00000158 0. 40 140 3 'M. not starts accidentally' 'yes' 'no'

:Closing the mold by pressing the intermittently button
40 0.00133 0. 45 150 3 'Op. uses the intermittently button' 'yes' 'no'

:Attach the mechanical safety of the slide of the press
45 0.0125 0. 50 150 3 'Op. put mechanical lock' 'yes' 'no'

:Enter security mechanical lock with key selector
50 0.00133 0. 52 150 3 'Op. turn correctly the key' 'yes' 'no'

:Key selector integrity
52 0.000004 0. 55 145 3 'Key selector works correcly' 'yes' 'no'

:Unlock the upper and lower mold halves with appropriate tools
55 0.0125 0. 60 135 3 'Op. acts correctly' 'yes' 'no'

:Place the new mold
60 0.00125 0. 62 135 3 'Op. acts in correct way' 'yes' 'no'

:Lock the two mold halves
62 0.0125 0. 65 65 3 'Op. lock the two mold halves' 'yes' 'no'
20 135 0.000003 1
```

:Recovery of the safe guards
65 0.01 0. 67 70 3 'Op. restores the safe guards' 'yes' 'Op. omits'
20 140 0.0000009 1

:Recovery of the safe guards in correct position
67 0.01 0. 70 70 3 'Correct distance transmitter and receiver' 'yes' 'no'
20 140 0.0000009 1

:Check operating selector
70 0.0125 0. 72 72 3 'Op. checks operating selector' 'yes' 'no'
20 106 0.00000008 1

:Test controls
72 0.0125 0. 75 75 3 'Op. tests anti repeat device' 'yes' 'no'
20 106 0.0000001 1

:Test control
75 0.0125 0. 77 77 3 'Op. tests protection accidental activation' 'yes' 'no'
20 106 0.0000001 1

:Test stop control
77 0.0125 0. 80 195 3 'Op. tests stop control' 'yes' 'no'

:Check good condition of perimeter protection
80 0. 0. 82 195 3 'Op. checks condition of perimeter protection' 'yes' 'no'
20 82 0.014 1

:Check guards securely fastened in place, no access possible to danger zone'
82 0.0125 0. 85 195 3 'Op. checks no access to danger zone' 'yes' 'no'

:Verify the absences of others in the vicinity of the press
85 0.0125 0. 86 145 3 'Op. verifies' 'yes' 'no'

:Vicinity of the press
86 0.03 0. 87 145 3 'No one near press' 'yes' 'no'

:Test 2-hand controls
87 0.003 0. 90 195 3 'Op. trials stroke with safe guards in place' 'yes' 'no'
20 105 0.000002 1

:Record data and test results
90 0.003 0. 100 195 3 'Op. records test results' 'yes' 'no'

:Put metal sheet in fixture
100 0.003 0. 105 150 3 'M. sheet properly positioned' 'yes' 'no'

:Simultaneous pressure and kept up launchers to run the process
105 0.0000011 0. 106 107 3 'Simultaneous device works correctly' 'yes' 'no'

:Accidental start of the actuator
106 0.0000000769 0. 140 107 3 'Command starts in an acc. way' 'yes' 'no'

:By-pass the device
107 0.0032 0. 140 110 3 'Op. by-passes device' 'yes' 'no'

:Remove formed part
110 0.0000000769 0. 140 115 3 'Accidental restart of the machine' 'yes' 'no'

:Place part in bin on floor
115 0.006 0. 120 200 3 'Op. put part in correct container' 'yes' 'no'
23 200 0 0

:Collect waste processing with special mean
120 0.0124 0. 205 125 3 'Op. uses special means' 'yes' 'no'
13 205 0 0

:In the case operator has to use hands disconnect the power supply
125 0.0125 0. 150 150 3 'Op. disconnects power supply' 'yes' 'no'
13 150 0 0

:Gravity fall of the mold
135 0.00000158 0. 150 190 3 'mold fall' 'yes' 'no'
13 150 0 0
24 190 0 0

:Light barrier
140 0.0000000554 0. 190 150 3 'l.b. intervines' 'yes' 'no'
14 190 0 0

:Dangerous actions, it is reccomended to stop the operation
145 0.0125 0. 150 150 3 'Stop operation' 'yes' 'no'
10 150 1 1

:Increase probability of injury for the operator
150 0. 0. 155 190 3 'Contact with tools' 'yes' 'no'
24 190 0 0

:Dynamics of injury for the operator
155 0.15 0. 160 190 3 'Hurt' 'no' 'yes'
23 190 0 0

:Dynamics of injury for the operator
160 0.27 0. 165 190 3 'Crushing' 'no' 'yes'
23 190 0 0

:Dynamics of injury for the operator
165 0.58 0. 170 190 3 'Cutting' 'no' 'yes'
23 190 0 0

:Dynamics of injury for the operator
170 0.37 0. 190 190 3 'Upper limb amputation' 'no' 'yes'
14 190 0 0
23 190 0 0

:Injury to the operator
190 1 0. 0 0 3 'Op. injured' 'yes' 'no'

:Machine is not under control
195 1 0. 0 0 3 'Machine under control' 'yes' 'no'

:Production Losses
200 1 0. 0 0 3 'Prod. losses' 'yes' 'no'

:Correct management waste
205 1 0. 0 0 3 'Ok collect waste' 'yes' 'no'

12.5.2 File source to verify Operational SIL related to light barrier.

```
:Light barrier
1 0.0000000911 0. 10 40 3 'l.b. works' 'yes' 'no'
24 40 0 0

:Recovery of the safe guards
10 0.000039 0. 20 40 3 'Op. restores the safe guards' 'yes' 'Op. omits'
24 40 0 0

:Recovery of the safe guards in correct position
20 0.000069 0. 30 40 3 'Correct distance transmitter and receiver' 'yes' 'no'
24 40 0 0

:By-pass the device
30 0.00077 0. 40 40 3 'Op.no by-passes device' 'yes' 'no'
13 40 0 0
24 40 0 0

:Availability of light barrier
40 1 0. 0 0 3 'l.b. available' 'yes' 'no'
```